

# Tainted Leaks Disinformation and Phishing With a Russian Nexus

---



[citizenlab.ca/2017/05/tainted-leaks-disinformation-phish/](https://citizenlab.ca/2017/05/tainted-leaks-disinformation-phish/)

May 25, 2017

*“Every external operation is first and foremost a domestic one: the single most important role of the agencies is to secure the regime.” — Mark Galeotti on Russian foreign intelligence*

## Key Points

---

- Documents stolen from a prominent journalist and critic of the Russian government were manipulated and then released as a “leak” to discredit domestic and foreign critics of the government. We call this technique “tainted leaks.”
- The operation against the journalist led us to the discovery of a larger phishing operation, with over 200 unique targets spanning 39 countries (including members of 28 governments). The list includes a former Russian Prime Minister, members of cabinets from Europe and Eurasia, ambassadors, high ranking military officers, CEOs of energy companies, and members of civil society.
- After government targets, the second largest set (21%) are members of civil society including academics, activists, journalists, and representatives of non-governmental organizations.
- We have no conclusive evidence that links these operations to a particular Russian government agency; however, there is clear overlap between our evidence and that presented by numerous industry and government reports concerning Russian-affiliated threat actors.

## Summary

---

This report describes an extensive Russia-linked phishing and disinformation campaign. It provides evidence of how documents stolen from a prominent journalist and critic of Russia was tampered with and then “leaked” to achieve specific propaganda aims. We name this technique “tainted leaks.” The report illustrates how the twin strategies of phishing and tainted leaks are sometimes used in combination to infiltrate civil society targets, and to seed mistrust and disinformation. It also illustrates how domestic considerations, specifically concerns about regime security, can motivate espionage operations, particularly those targeting civil society. The report is organized into four parts described below:

**PART 1: HOW TAINTED LEAKS ARE MADE** describes a successful phishing campaign against David Satter, a high-profile journalist. We demonstrate how material obtained during this campaign was selectively released with falsifications to achieve propaganda aims. We then highlight a similar case stemming from an operation against an international grantmaking foundation, headquartered in the United States, in which their internal documents were selectively released with modifications to achieve a disinformation end. These “tainted leaks” were demonstrated by comparing original documents and emails with what Russia-linked groups later published. We conclude that the tainting likely has roots in Russian domestic policy concerns, particularly around offsetting and discrediting what are perceived as “outside” or “foreign” attempts to destabilize or undermine the Putin regime.

**PART 2: A TINY DISCOVERY** describes how the operation against Satter led us to the discovery of a larger phishing operation, with over 200 unique targets. We identified these targets by investigating links created by the operators using the Tiny.cc link shortening service. After highlighting the similarities between this campaign and those documented by previous research, we round out the picture on Russia-linked operations by showing how related campaigns that attracted recent media attention for operations during the 2016 United States presidential election also targeted journalists, opposition groups, and civil society.

**PART 3: CONNECTIONS TO PUBLICLY REPORTED OPERATIONS** outlines the connections between the campaigns we have documented and previous public reporting on Russia-linked operations. After describing overlaps among various technical indicators, we discuss the nuance and challenges surrounding attribution in relation to operations with a Russian nexus.

**PART 4: DISCUSSION** explores how phishing operations combined with tainted leaks were paired to monitor, seed disinformation, and erode trust within civil society. We discuss the implications of leak tainting and highlight how it poses unique and difficult threats to civil society. We then address the often-overlooked civil society component of nation-state cyber espionage operations.

## Introduction: Tainted Leaks & Civil Society Targets

---

Russia-linked cyber espionage campaigns, particularly those involving targeting around the 2016 U.S. elections, and more recently the 2017 French election, have dominated the media in recent months. As serious as these events are, often overlooked in both media and industry reports on cyber espionage is a critical and persistent victim group: global civil society.

A healthy, fully-functioning, and vibrant civil society is the antithesis of non-democratic rule, and as a consequence, powerful elites threatened by their actions routinely direct their powerful spying apparatuses toward civil society to infiltrate, anticipate, and even neutralize their activities. Unlike industry and government, however, civil society groups typically lack resources, institutional depth, and capacity to deal with these assaults. For different reasons, they also rarely factor into threat industry reporting or government policy around cyber espionage, and can be the silent, overlooked victims.

As with previous Citizen Lab reports, this report provides further evidence of the “silent epidemic” of targeted digital attacks on civil society, in this case involving widely reported Russian-affiliated cyber espionage operations. Our report underscores the domestic roots of these foreign operations, and how concerns over regime security and domestic legitimacy can factor into Russian threat modeling and espionage targeting, both at home and abroad.

## Patient Zero for the Investigation: David Satter

---

Our investigation began with a single victim: David Satter, a high-profile journalist, Rhodes Scholar, and critic of the Kremlin. In 2013, Satter was banned from Russia, allegedly for “flagrant violations” of visa laws, but which most attribute to his investigative reporting on Russian autocracy. Satter is known for his book, *Darkness at Dawn*, which investigated the possible 1999 conspiracy involving the Russian Federal Security Service (FSB) in a series of bombings of Russian apartment buildings that was used as a justification for the second Chechen War and which facilitated the rise to power of Vladimir Putin.

On October 7, 2016 Satter fell victim to a targeted phishing campaign, and mistakenly entered his password on a credential harvesting site. Satter’s e-mails were stolen and later published selectively, and with intentional falsifications, as we will describe in this report. While we cannot conclusively attribute the theft of Satter’s emails to one particular threat actor, nor do we have concrete details on the process by which his stolen emails were falsified and made their way into the public domain, we uncover and analyze several pieces of evidence to help contextualize the tainted leaks, while at the same time linking the infiltration of his email to a much wider cyber espionage campaign that has a Russian nexus.

## Tainted Leaks: Disinformation 2.0

---

Following the compromise of his account, Satter’s stolen e-mails were selectively modified, and then “leaked” on the blog of CyberBerkut, a self-described pro-Russian hacktivist group. This report introduces the term “tainted leaks” to describe the deliberate seeding of false information within a larger set of authentically stolen data.

We examine in detail how a report sent to the National Endowment for Democracy (NED) about *Radio Liberty*’s Russian investigative reporting project (contained in the emails stolen from Satter) was carefully modified with false information prior to being released. We show how this manipulation created the false appearance that prominent Russian anti-corruption figures, including Alexei Navalny, were receiving foreign funding for their activities. (Alexei Navalny is a well-known Russian anti-corruption activist and opposition figure). We also note how the document was used in an effort to discredit specific reports about corruption among close associates of Russian President Vladimir Putin.

In addition, whoever tainted the document also made reference to an article that had not yet been published at the time the document was “leaked.” This timing strongly suggests advance knowledge of the publication of an upcoming piece of investigative journalism concerning

senior Russian officials and businessmen. Such information is likely to have been sensitive, and would not have been widely known. This may suggest that the operators had access to other, ongoing surveillance operations.

Once the tainted leak was released, Russian state-owned media and others reported that the document showed a CIA-backed conspiracy to start a “colour revolution” in Russia.<sup>1</sup> The tainted leak was also reported as evidence that the reports on corruption within Putin’s inner circle represented part of a deliberate disinformation campaign on behalf of foreign interests.

The timing and substance of the tainting coincides with reported fears among Putin and his close associates that revelations about their wealth and its sources could trigger protests and uprisings within Russia, like those led by Navalny in recent months and years.

Tainted leaks pose complex challenges to the victims of breaches, as well as representing a potent and troubling method of disinformation. **Part 1** describes the leak tainting in greater detail, and **Part 4: Discussion** provides an analysis of the risks posed by the tactic.

## Pandora’s Un-Shortening: High Value Targets Emerge

---

While investigating the suspicious messages sent to Satter, we determined that Tiny.cc, the link-shortening service used by the operators to phish credentials, had predictable features that enabled us to discover some other links likely used by the same operators. We developed a technique to discover some of these links, and ultimately collected 223 malicious links representing 218 unique targets.<sup>2</sup> We have been able to identify the real identity of approximately 85% of the targets. Of the set we identified, we found targets from at least 39 countries.

One thread that links the targets is that their professional activities connect them to issues where the Russian government has a demonstrated interest. In some cases, the targets are Russians, ranging from an ex-Prime Minister, to journalists who investigate corruption, to political activists. Many more targets are from, posted to, or involved in extractive industries in countries and areas where the Russian government has an economic and strategic interest, such as former Soviet states. Still others are likely to be working on issues on the other side of the negotiating table from Russia, whether as part of United Nations operations, NATO, or civil service. Perhaps unsurprisingly, one of the largest groups of targets are high-ranking military and government personnel and elected officials in Ukraine.

# TAINTED LEAKS: TARGETS LINKED TO 39 COUNTRIES

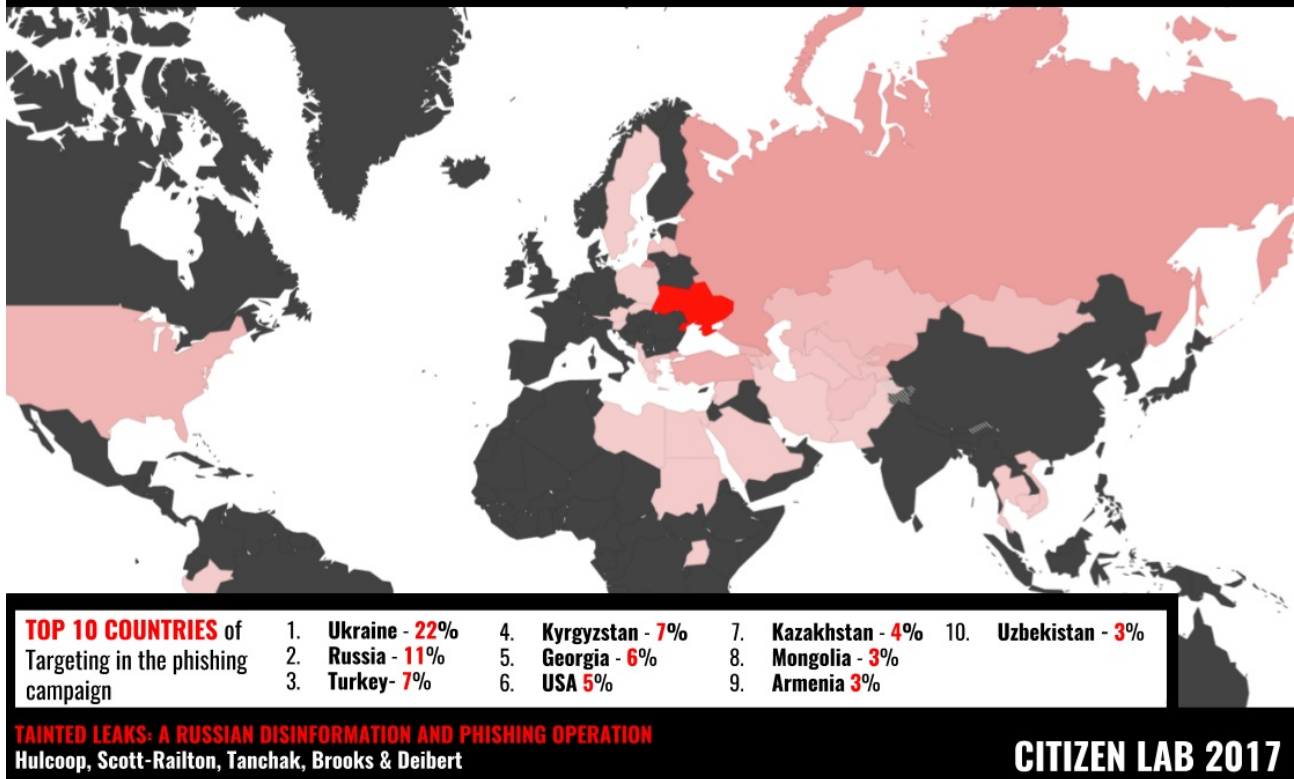


Figure 1: Map showing countries that targets of the phishing campaign are linked to [click for hi-res]

In other cases, for instance, the wife of a military attache, individuals appear to be targeted because of their proximity to high value targets. In others, we have identified a large number of individuals who appear to be targeted because they received support, in the form of a fellowship, from a particular US-based grantmaker.

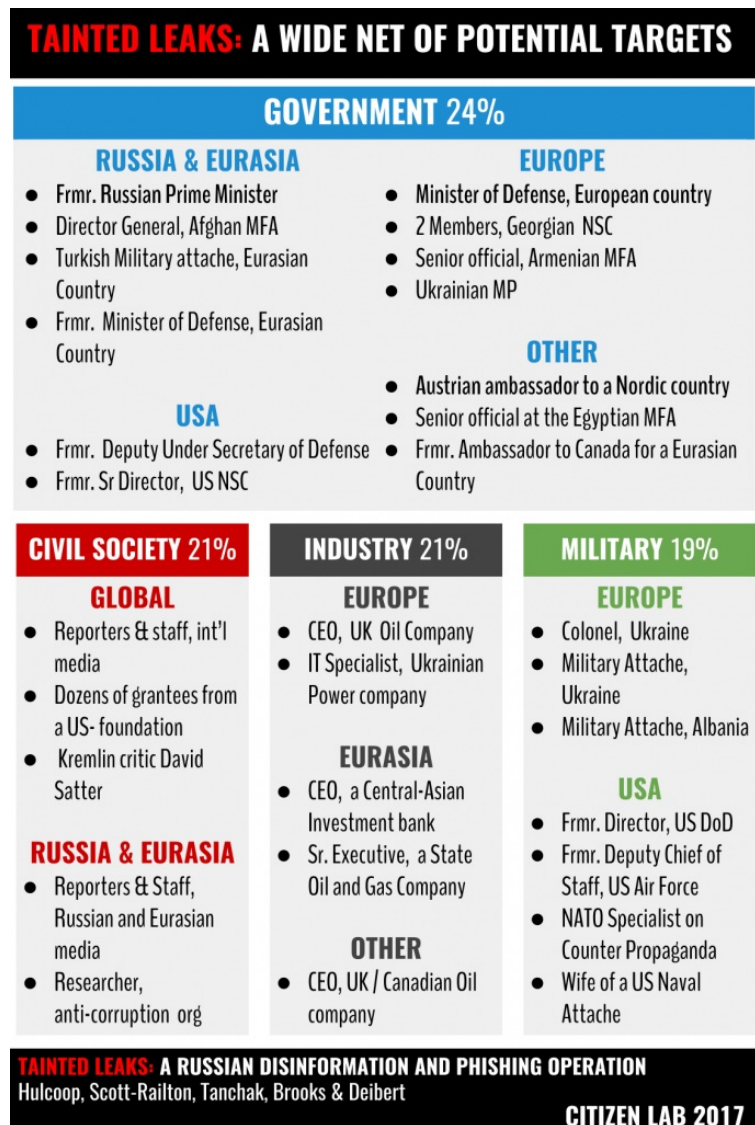
Some notable target categories include:

- Politicians, public servants and government officials from Afghanistan, Armenia, Austria, Cambodia, Egypt, Georgia, Kazakhstan, Kyrgyzstan, Latvia, Peru, Russia, Slovakia, Slovenia, Sudan, Thailand, Turkey, Ukraine, Uzbekistan and Vietnam
- Diplomatic personnel from numerous embassies, up to and including ambassador level, as well as their family members
- Civil society members including very high profile critics of the Russian president, as well as journalists and academics
- Senior members of the oil, gas, mining, and finance industries of the former Soviet states
- United Nations officials
- Military personnel from Albania, Armenia, Azerbaijan, Georgia, Greece, Latvia, Montenegro, Mozambique, Pakistan, Saudi Arabia, Sweden, Turkey, Ukraine, and the United States, as well as NATO officials



The discovery of so many other targets provides us with a window into the campaign's structure, and objectives (**Part 2** outlines how we discovered the targets). After government targets, the second largest set (21%) are members of civil society like academics, activists, journalists, and representatives of non-governmental organizations.

Figure 2: Some high-value targets who received phishing emails



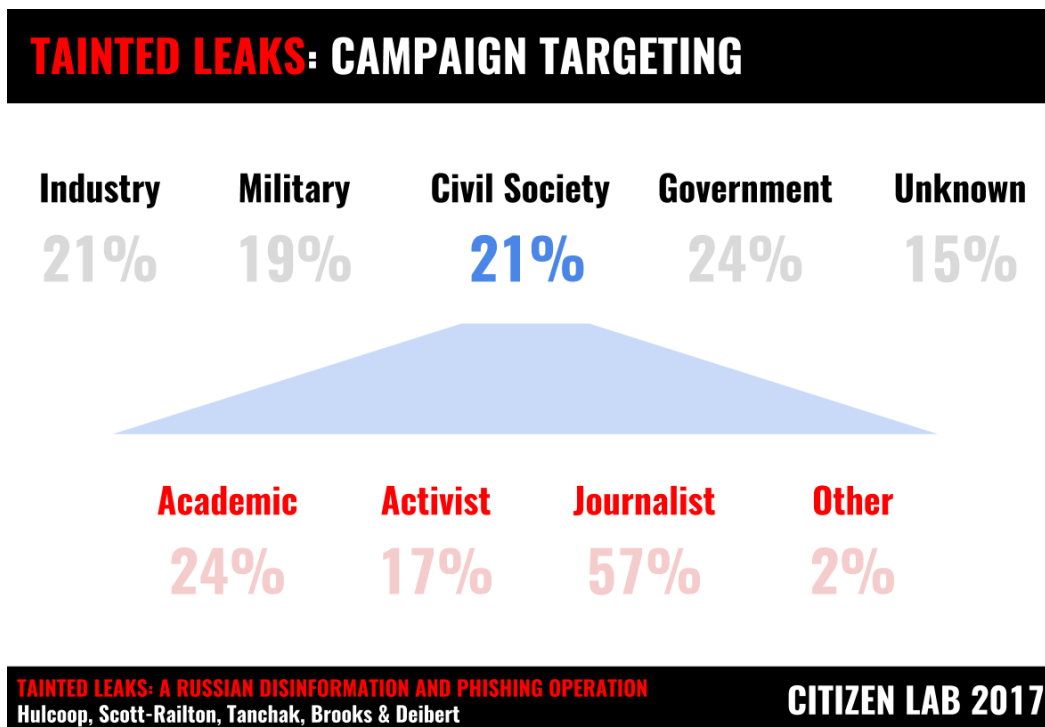
## The Importance of Civil Society Targets

The data presented in Figure 3 underscore the extent to which civil society groups are being targeted in numbers equivalent to those seen with the more classic 'cyber espionage' sector-aligned targets such as military, government, and industry.

Amongst the civil society targets, more than half were journalists, many of whom are prominent contributors to Russian language news outlets such as Vedomosti, Slon/Republic, Novaya Gazeta, and the BBC Russian Service.

While providing a detailed analysis of the civil society targets or an outline of their areas of activity would undoubtedly jeopardize their privacy, we can safely reflect on two notable patterns that emerge from such an analysis.

The first is that, like our first subject David Satter, several individuals from the target list were known for their public efforts towards shining a light on the Russian government and its activities. From publishing articles that outline fraud or corruption, to general activism in support of electoral reform, many of the civil society targets seem to have been singled out for the perception that their actions could pose a threat to the Putin regime.



**Figure 3: Breakdown of discovered targets into broad categories**

Another notable commonality found during analysis of the civil society targets of these campaigns is the near perfect alignment between their areas of activity and the geopolitical conflicts in which Russia is a known or suspected belligerent, or party to the conflict.

Specifically, the focus areas of the civil society targets span geographic boundaries, including conflict areas such as Syria, Afghanistan, Ukraine, and others.

We also found that several dozen of the targeted individuals had as a thread in common that they had received a fellowship from a single funder focused on the region.

## Notification

The large and diverse target group presented notification challenges. Our process for notifying potential victims involved the following considerations and steps:

- For targets affiliated with governments or government-affiliated organizations (such as NATO or the United Nations), or businesses in a particular country, we passed information on targets' names and email addresses to the relevant Computer Emergency Response Team (CERT)
- If many targets shared an organizational affiliation, but not a single employer, we contacted that organization and worked with them to notify the individuals

- We also provided a full list of targets to the targets' e-mail provider.

## Part 1: How Tainted Leaks Are Made

---

*We examine how stolen materials from Satter's inbox were turned into tainted leaks and released by CyberBerkut, and then examine a similar operation against the Open Society Foundations.*

To make a clean comparison between real and fake, and illustrate exactly how tainting takes place, we obtained original, genuine documents and e-mails from David Satter, a victim of a breach, and compared them with the tainted versions. We then describe a prior case of tainted leaks: internal documents belonging to the Open Society Foundations were stolen, then later released with tainting similar to Satter's, also by CyberBerkut.<sup>3</sup>

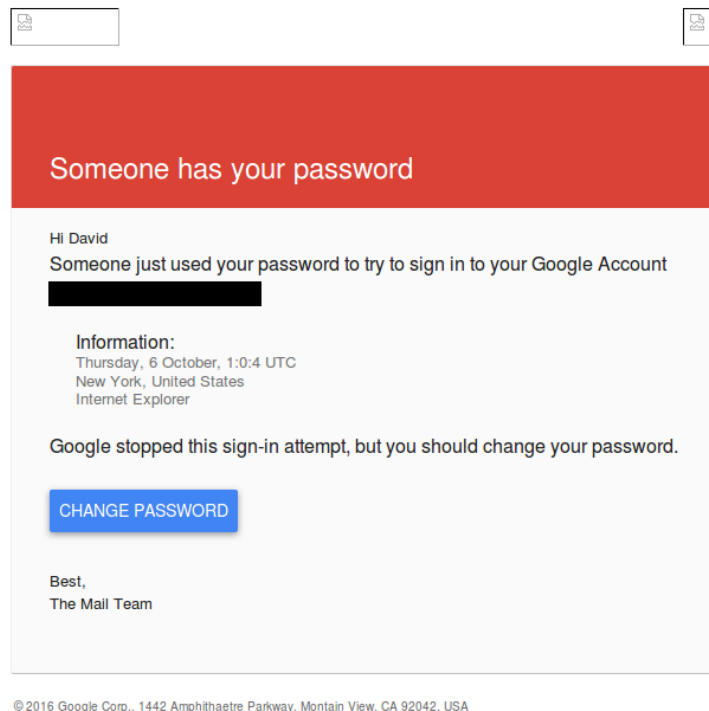
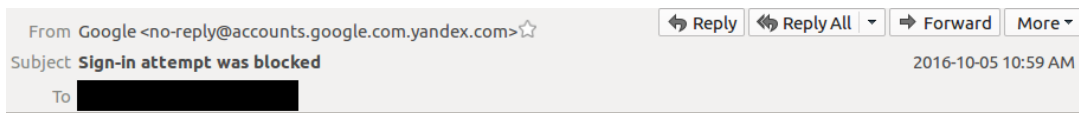
In both cases the breach victims were working with US-based organizations which had programs specializing in Russia. The tainting appeared to have two objectives: cause the programs to appear more subversive of Russia than they were, and discredit specific opposition individuals and groups critical of Russian President Putin and his confidants.

### The Case of David Satter

---

On October 5, 2016, a phishing email was sent to the Gmail address of David Satter (See: **Patient Zero: David Satter**). This phishing email was crafted with a specific ruse designed to look like a security warning from Google, suggesting to the recipient that an unknown third-party has obtained their Gmail account password (see Figure 4).





**Figure 4: Phishing Email 1, mimicking a genuine message from Google**

The phishing email is designed to trick the recipient into clicking on the 'Change Password' button. Clicking on this link would direct the victim's web browser to a link hosted on the URL shortening service Tiny.cc. The operator disguised the link by using an open redirect hosted by Google. This open redirect allowed the operators to create a URL that, superficially, appears to be hosted by Google:

[https://www.google.com/amp/tiny.cc/\(redacted\)](https://www.google.com/amp/tiny.cc/(redacted))

Unfortunately, the ultimate destination of this shortened URL was changed to a benign webpage before we were able to examine this phishing email. However, as we will outline in **Part 2** of this report, there is sufficient evidence available to suggest the original destination.

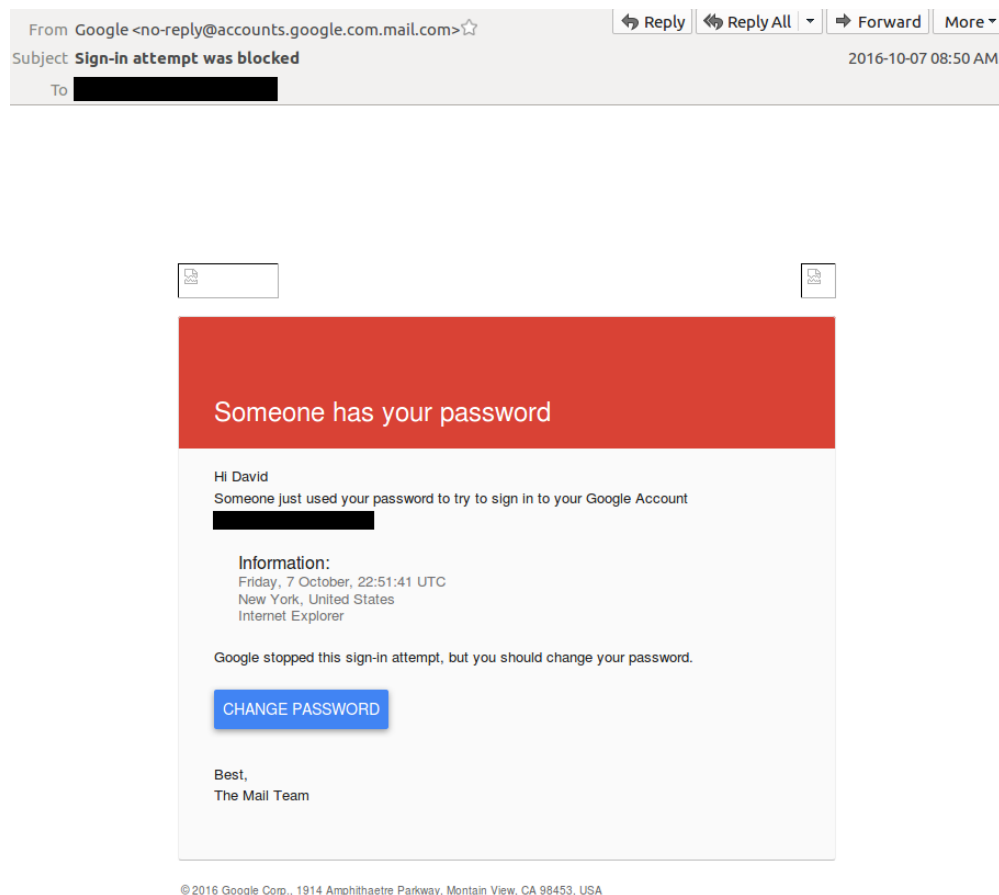
Analysis of the email headers revealed that the message was sent with the Russian email service Yandex, using email account *g.mail2017[@]yandex.com*.

## A Second Phishing Email

Two days later, on October 7, 2016, Satter received a second email that used an identical deception to the first attempt detailed above.

As with Email 1, the google.com/amp/ redirect pointed to a URL hosted by Tiny.cc. Once again, similar to Email 1, Citizen Lab found that the originally configured redirection target for this link had been removed.

Analysis of the email headers in this second phishing attempt show that the message was sent with the web-based email service 'mail.com', using email account *annaablony[ @ ]mail.com*.



**Figure 5: Phishing Email 2**

## Unauthorized Access

On October 7 2016, shortly after receiving the email, Satter reports having clicked on the change password link in Email 2, and recalls being redirected to what he now realizes was in fact a credential phishing page which appeared to be a legitimate Google sign-in page.

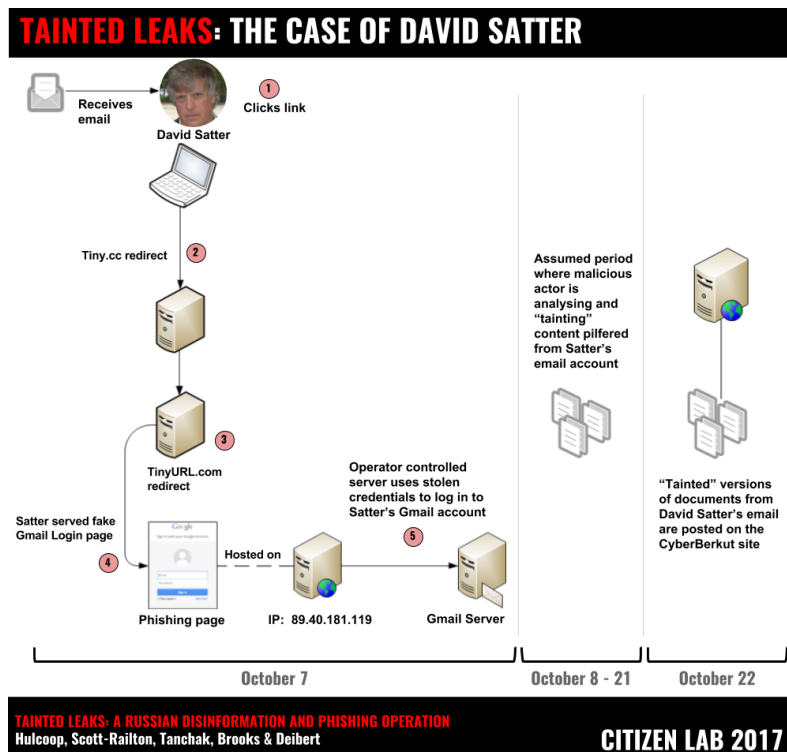
Unfortunately, Satter had temporarily disabled 2-factor authentication on his account, making the compromise possible.

Shortly after entering his credentials, Satter's Gmail [account activity](#) page recorded an unauthorized login event. The data logged by Google indicated that the login session originated from an IP address in Romania (Figure 6). In **Part 2** we will show that the server associated with this IP address was also hosting the fake Google login page where Satter submitted his account credentials. Thus it is likely that this malicious server was configured to automatically download the email contents from any compromised accounts (see Figure 7).

**Figure 6: Screen grab from Google account activity page**

In **Part 2** of this report we will outline how the phishing links sent to Satter led us to discover a much wider campaign that included 218 distinct targets from government, industry, military, and civil society. In the following section, we provide context concerning the disinformation campaign that was conducted around material stolen from Satter's email account and published on the blog of CyberBerkut, a pro-Russian hacktivist collective.

Time:	October 7, 2016 2:46pm
Location:	Bucharest, Romania
IP address:	89.40.181.119 ?



**Figure 7: How a phishing campaign against Satter became a tainted leaks operation**

## Analyzing a Tainted Leak

*This section compares an original document obtained by Citizen Lab with a tainted document published online, and used as part of a disinformation campaign. We describe the tainting in detail, and analyse the likely objective.*

Several documents from Satter's emails were posted by CyberBerkut at the same time without observable manipulation. However, one document showed extensive evidence of tainting. The tainted leak was a report authored by Satter describing Radio Liberty's Russian Investigative Reporting Project. The document was modified to make Satter appear to be paying Russian journalists and anti-corruption activists to write stories critical of the Russian Government. Importantly, we do not know the process through which the stolen document made its way from Satter's inbox to the CyberBerkut release. In the CyberBerkut version, the document is posted as screen-captures, and thus lacks metadata.



**Figure 8: CyberBerkut post dated October 22, 2016 showing the narrative accompanying the tainted leak document (highlighted with arrow). [Archived copy]**

The original document lists a series of articles from *Radio Liberty* exclusively that are part of the project. The articles concern a range of topics: history, economics, and politics. *Radio Liberty* is a U.S. government international broadcaster, founded in 1951 to broadcast news and information into the Soviet Union. It merged with *Radio Free Europe* in 1976, who now together are incorporated as a 501(c)(3), funded and overseen by the United States' Broadcasting Board of Governors.

The tainted document modifies the text to appear to be a report on a much larger (nonexistent) project to pay for articles by a range of authors, which would subsequently be published by a range of media outlets. The deceptively inserted articles, almost all of which are genuine publications, focus on corruption within Putin's friends and inner circle. The work of Alexei Navalny, a prominent Putin critic, is repeatedly emphasized. The full tainted document is in **Appendix A**.

## Taint 1: Making reporting look like a secret influence operation

The operators modified the document's scope in an attempt to create the appearance of a widespread media campaign. They did this by removing or modifying mentions of *Radio Liberty* throughout the document.

**The Radio Liberty** Russian investigative reporting project is gaining traction and producing significant journalism **for the site of the Radio Liberty Russian Service**. In this way, it is making a contribution to Western efforts to provide the Russian population with objective information.

**Figure 9: Text in red was removed, creating the impression of a wide media campaign, not the programming of a specific news source.**

Other content, such as discussions of specific translators working for *Radio Liberty* are similarly removed to preserve the fiction.

Of the articles that have been published ~~on in~~ the Russian ~~site media~~, four have been translated into English and published on the site of the Henry Jackson Society. These are the articles about Rogozin, Gaydamuk, Chemezov and Russian space exploration. ~~A backlog of articles to be translated has developed because Arch Tait, our translator, had to take a break to work on the translation of a book. He is now back at work and will begin translating some of the pieces.~~ Still to be worked out, however, are arrangements for publishing these pieces ~~in English on the English Language~~ site of Radio Liberty. David Satter will be traveling to Prague in late October during which time he hopes to

**Figure 10: The document was further tweaked to create the impression of a larger campaign. A note about a translator was also removed as it would contradict the impression**

We believe that by removing specific references to *Radio Liberty*, the perpetrators are aiming to give the impression of a broader subversive campaign not limited to a single news organization. Doing so allows the perpetrators to falsely associate non-US funded organizations, such as independent NGOs, to appear to be linked as part of this larger, fictitious program.

We are seeking to expand our network of journalists and have had some success despite the risks of writing ~~for Radio Liberty without the protection of a full-time job~~ ~~articles~~. This effort will continue.

**Figure 11: Further tainting to remove mentions of Radio Liberty**

Finally, a clause is deleted at the end of the document concerning the risks of writing “without the protection of a full time job” (Figure 11). This deletion may simply be the tainters removing an inconvenient sentence that refers to *Radio Liberty*, but it also may be an attempt to make the activity look more “cloak and dagger.”

## Taint 2: Discrediting specific journalists and Kremlin critics

---

The original document included a list of 14 articles published as part of the Russian Investigative Project at Radio Liberty. The tainted document includes 24. The operators not only added to the list, but also tweaked the Radio Liberty articles to further the impression of a larger campaign.

18. Evgeny Gusev, “The King of State Orders,” September 5, 2016 [the corruption of Putin’s friends, the Rotenberg brothers] (RFE/RL)

19. Irina Dolinina and Alesya Marokhovskaya, “Journalists Have Found Analogues of the Ozero Cooperative All Over the Central Russia,” September 8, 2016 [corruption in the regions] (Slon)

20. Alexei Navalny, “There, Beyond the 6-Meter-High “fall of Medvedev’s Dacha,” September 15, 2016 [an investigation on prime minister Medvedev] (Navalny.com)

21. Alexei Navalny, “He is Putin’s Cook. He is Putin’s Troll. He is a Billionaire,” October 4, 2016 [the fate of Prigozhin, one of the businessmen close to Putin] (Navalny.com)

22. Maria Zholobova and Maria Borzunova, “Apartment Worth More than Half a Billion Was Found at Putin’s Ex-Bodyguard Samename,” October 9, 2016 [the corruption of Putin inner circle] (TV Dozhd)

---

23. Irina Gruzina, Ivan Vasiliev, Irina Skrynnik, “Samolet Development is Ready to IPO,” October 12, 2016 [about Moscow Oblast governor’s illegal business ties] (Vedomosti)

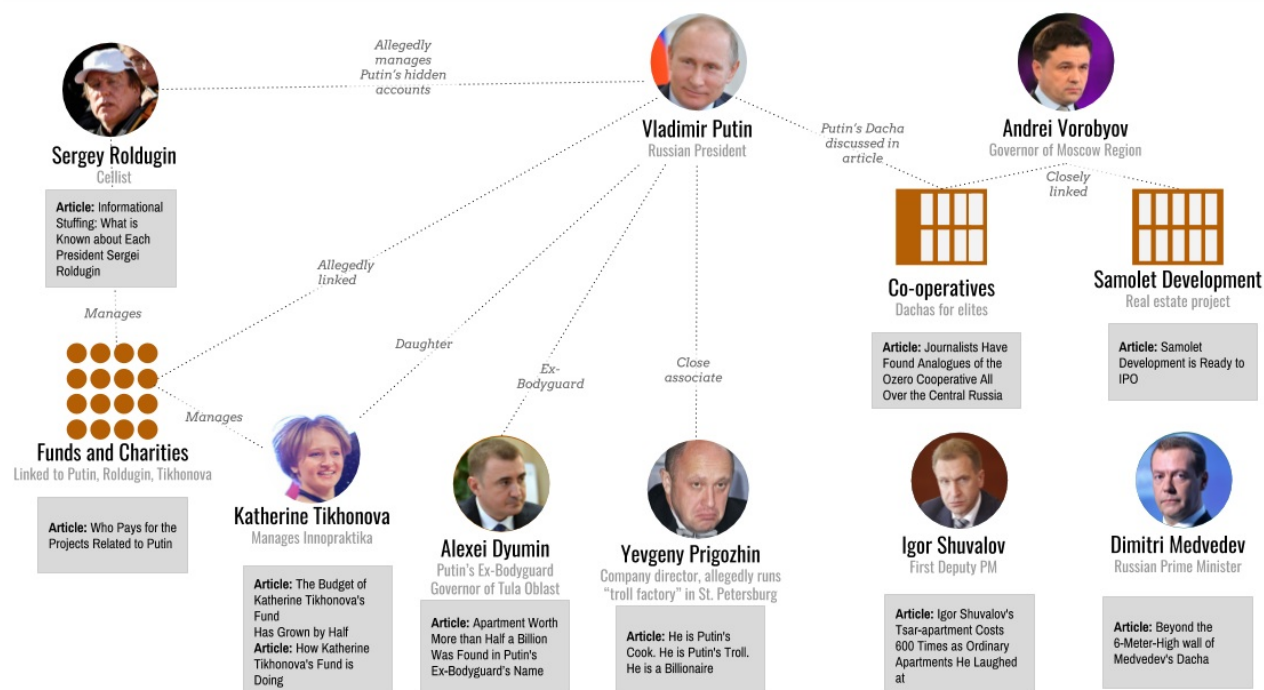
24. Alexei Navalny, “How Katherine Tikhonova’s Fund is Doing,” October 18, 2016 [the fund of Putin’s daughter] (Navalny.com)

**Figure 12: Six of the ten added articles. All blue text was added to the original as part of the tainting. The objective is to make these reports appear to have been supported by the project.**

Ten additional articles were added. Although the original list of publications covered a variety of themes, the added set primarily focuses on issues of corruption, and the wealth of those in Putin’s circle. The articles, written for a range of publications, all share a theme: corruption and personal enrichment by those close to Putin and the Russian Government (See Appendix A).



# TAINTED LEAKS: PEOPLE & TOPICS ADDED IN THE TAINTING



**TAINTED LEAKS: A RUSSIAN DISINFORMATION AND PHISHING OPERATION**  
Hulcoop, Scott-Railton, Tanchak, Brooks & Deibert

**CITIZEN LAB 2017**

Figure 13: People and Topics of articles added in the tainting. Images: Wikipedia, Radio Free Europe, Reuters [\[click for hi-res\]](#)

Of special interest are the insertions of Alexei Navalny, a prominent Russian anti-corruption activist and opposition figure whose work, and Anti-corruption Foundation, receives widespread domestic and international attention. By repeatedly adding his reporting to the document, the tainting creates the appearance of “foreign” funding for his work. This theme also figured prominently in the disinformation campaign surrounding the original publication, on October 22, 2016, of the tainted document by CyberBerkut (See: Disinformation Campaign Surrounding the Tainted Document).

## Taint 3: Claimed foreknowledge

An article by Russian journalist Elena Vinogradova describing issues involving “senior Russian officials and businessmen” was also added as part of the tainting, which goes on to state that it will be published by Russian-language news service Vedomosti on October 24-25.<sup>4</sup>

Soviet Union, by Galina Sidorova and an analysis of the structure of power and corruption in the Samara Oblast by Vladimir Voronov. **Besides, on October 24-25, Vedomosti columnist Elena Vinogradova will publish an article about Moscow Oblast issues in which senior Russian officials and businessmen close to Putin will be mentioned.**

Figure 14: Tainting that suggests the operators had advanced knowledge of a news report

This timing is significant as the original CyberBerkut publication of the tainted document occurred on October 22 2016, slightly before this date.

The apparent foreknowledge suggests that the individuals responsible for the tainting had advance knowledge of the content and publication date of a piece of investigative journalism, which may mean the operators had access to intelligence or surveillance reports concerning the activities of the Elena Vinogradova.

We identified at least one individual among the set of targets of the phishing campaign whose account might have provided this information, however we were not able to confirm a compromise.

Importantly, we were not able to find concrete evidence of the publication of an article matching the description added in the tainting. It is possible that existence of the article was a fabrication, or the result of misplaced speculation by the individuals responsible for the tainting.

#### Taint 4: Modifying the Time Frame and Supporting Details

---

The timeframe and number of publications are increased, perhaps to give the impression of a longer and more intense campaign. Changes are also made to accommodate a wide range of articles *not published by Radio Liberty* but by other parties.

In the first **nine ten** months of 2016, **fourteen twenty four** investigative or in depth articles have been published under aegis of the project. In addition, six other articles are in progress or are awaiting publication. The following is a list of the articles that were published as of **September 30-October 20**, 2016:

#### Figure 15: Dates and numbers changed to accommodate ten more articles

Text that mentions specific dates in the original document that would not accommodate the articles that have been falsely added is also changed to support the new fiction.

#### Disinformation Campaign Surrounding the Tainted Document

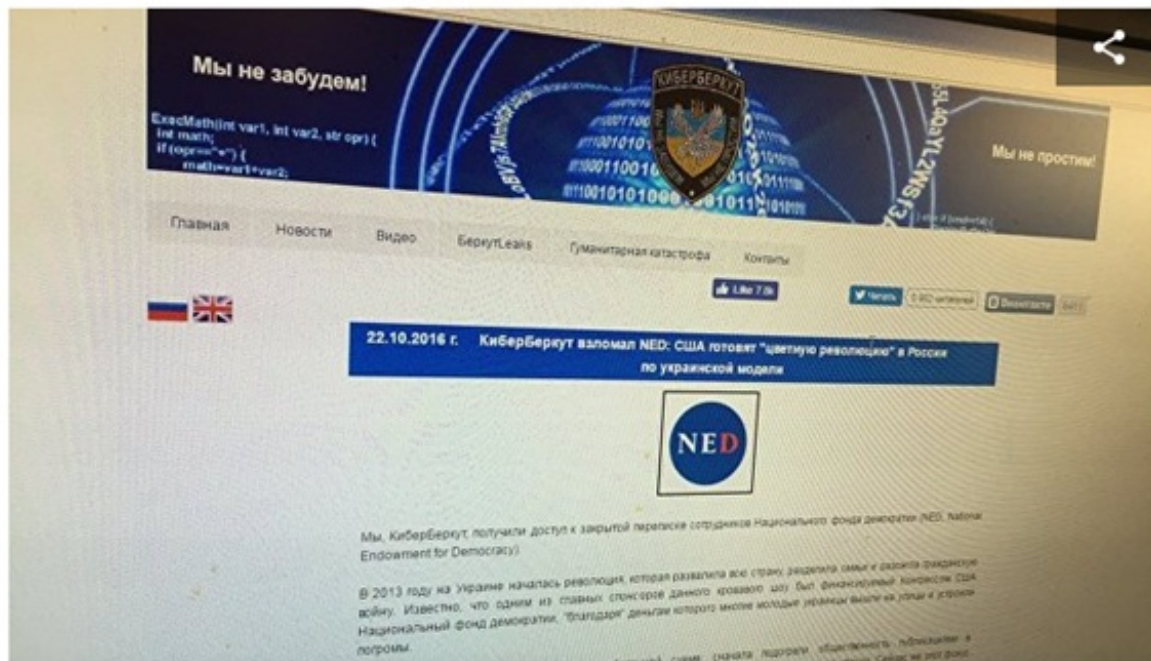
---

The tainted version of the stolen document was released online by CyberBerkut, which represents itself as a group of pro-Russian hacktivists. CyberBerkut provided the framing narrative for the tainted document in a post on October 22, 2016: they were releasing the document to provide evidence that the United States was attempting to support a “colour revolution” in Russia. In the CyberBerkut narrative, David Satter was an agent directing the publication of articles critical of the Russian government.

# Политолог о "цветной революции" в РФ: пора бы США подключить фантазию

12:39 24.10.2016 (обновлено: 13:47 24.10.2016)

26 9416 153 2



© РИА Новости / РИА Новости

**США хотят устроить в РФ "цветную революцию" по украинской модели, заявила хакерская группа "КиберБеркут". Политолог Михаил Смолин в эфире радио Sputnik отметил, что российское общество уже выработало иммунитет к подобным попыткам Вашингтона.**

**Figure 16: RIA Novosti, Russia's state operated news agency, reporting the Cyber Berkut's release of the tainted leaks**

Russia's state operated news agency *RIA Novosti*, as well as *Sputnik Radio*, picked up the narrative, and gave voice to a number of sources who claimed that the "leak" was evidence that the United States Central Intelligence Agency (CIA) was attempting to foment a "colour revolution." The document was cited in a *RIA Novosti* report as providing evidence of "over 20" reports intended to discredit the Russian president, and his entourage. The "colour revolution" narrative was echoed in [this SM News report](#), and by [Vesti.lv](#), among others.

Meanwhile, other Russian-language sources claimed that the document discredited Navalny's Anti-corruption Foundation by showing that its articles were actually ordered by David Satter.

## The Open Society Foundations Case

In 2015, the Open Society Foundations (OSF) experienced a breach of confidential data.

The redundant releases enable a comparison of documents between the two leaks using public materials. The DC Leaks dump included the release of untainted stolen documents that had been previously released as part of a tainted leak by Cyber Berkut. An [article in Foreign Policy](#) used this dump to identify several cases of leak tainting. We were able to verify each of their observations, as well as identifying additional elements of tainting.

As with the Satter case, the tainting appears to have a primarily domestic focus, and to be aimed at de-legitimizing figures like Navalny by making it appear that they are the recipients of illicit, foreign funding. This is a view that Navalny, one of the targets of the tainting, has also [expressed to Foreign Policy](#).

First, CyberBerkut released a tainted budget document to make it appear as if OSF was funding Alexei Navalny's Foundation for Fighting Corruption.

[illegible]

The tainters may have been working quickly, resulting in a small error, in which a dollar amount was substituted for “Approved Date.”

Second, a proposed funding strategy document was similarly modified to include the Foundation for Fighting Corruption in a list of groups to receive OSF support.



b.) Access to Alternative Information:

Russia remains bereft of a dense set of institutions that focus analytically on issues of policy relevance. Such organizations – including the Levada Center, the premier independent polling agency; the Carnegie Moscow Center, a leading independent think tank; **Foundation for Fighting Corruption, a leading anti- corruption source**; and SOVA, a source of expert research and analysis on hate speech and xenophobia – are instrumental in providing alternative and independent information to Russian society. Their work is utilized by policy experts,

**Figure 18: Proposed Strategy Document showing the location where the tainted document is modified to include mention of the Foundation for Fighting Corruption**

The tainting resumed later in the document, when several media outlets (*Echo Moscow*, *RosBusinessConsulting*, and *Vedomosti*) were also added to the document, apparently to create the perception that they had received the support of OSF.

media has become an essential tool for Russia’s intellectual communities. Activists, experts, and academics all make use of online platforms to discuss and debate topics not covered in traditional media, ranging from police abuse to the politicization of history textbooks. These online discussions – whether via a Facebook community page, a LiveJournal blog, **via support of liberal media like Echo Moscow, RosBusinessConsulting, Vedomosti newspaper** or an analytical news **site sites** like Polit.ru **and other** – can be a powerful force for influencing Russian public opinion on key issues of the day.

**Figure 19: A second section in the same document showing once more how several media outlets, including Echo Moscow, RosBusinessConsulting, and Vedomosti have been added.**

The second instance of tainting in the strategy document also introduced a slight grammatical error when the tainters neglected to remove “an” before changing “news site” to the plural “news sites.”

## Document Addressing the NGO Law

---

Finally, in a document addressing grantees and Russia’s NGO law, tainting was again performed to add Navalny’s Foundation for Fighting Corruption. The tainting also purported to show the foundation receiving money via Yandex, a widely-used Russian platform offering an online payment service.

ORG Name	Will Register as Foreign Agent	Will Not Register as Foreign Agent	Will take foreign funds	Will NOT take foreign funds	Undecided	Notes
Za Prava Cheloveka (Lev Ponamarev)		X	X – but indirectly			Constitutional Court, civil disobedience. Sent letter w/ MHG to USG asking if we are foreign agents; received reply from State that they are not.  Would receive foreign funds but via International University, not directly. Has received significant state funding.
Civil Assistance (Gannushkina) Foundation for Fighting Corruption (Navalny)		X	X			Constitutional Court, ECHR Funding via Yandex.Money E-wallet method
International Memorial (Roginsky)		X	X			Press release indicating that

**Figure 20: Tainted document, once more showing the addition of Navalny's Foundation for Fighting Corruption**

Taken together, both the tainted document stolen from David Satter, and the tainted OSF documents paint a picture of a competent adversary working to achieve several objectives, including discrediting domestic critics of Russia's government and president, while simultaneously attempting to embarrass foreign funders with activities in Russia. In **Part 4** we discuss the significance of tainted leaks as a disinformation technique.

## Part 2: A Tiny Discovery

*Beginning with the shortened link sent to David Satter, we identified a predictable feature in how the link shortener (Tiny.cc) generated its shortened URLs. This enabled us to identify over 200 additional targets of the same operation described in **Part 1**. This section describes the process used to enumerate these targets, and further describes the links between this operation and other publicly-reported Russian-linked phishing campaigns.*

In September 2016, ThreatConnect published a [blogpost](#) documenting phishing attempts against contributors to the citizen journalism website Bellingcat and its founder Eliot Higgins. The targeted contributors were actively engaged in reporting on the Russian involvement in the July 17, 2014 downing of Malaysia Airlines Flight 17. ThreatConnect attributed these intrusion attempts to [Fancy Bear](#) (aka [APT28](#)), a threat actor widely believed to be directly linked to the Russian government. In an October update to this post, ThreatConnect documented an additional spear phishing attempt against a Bellingcat contributor.

This latest credential phishing attempt was largely similar to the first email sent to David Satter (see **Part 1**, The Case of David Satter). Both emails were sent at 10:59am EST using the same sending address: [g.mail2017\[@\]yandex.com](#). In addition, both shared a fake Gmail footer that was distinctively modified from Gmail's original footer.



**Figure 21: Footer from the phishing emails sent to Bellingcat and David Satter showing a distinctive misspelling (possibly to avoid spam filtering)**

In both cases the malicious links embedded in these phishing emails were configured to redirect the targets to addresses hosted on the URL shortening service Tiny.cc. As ThreatConnect showed, the Tiny.cc link used against the Bellingcat contributor actually redirected the victim to another shortened URL, this one hosted by a different shortening service: TinyURL.com. Ultimately, this series of link redirections led to a malicious credential phishing page hosted at the following URL:

hxxp://myaccount.google.com-changepassword-securitypagesettingmyaccountgooglepagelogin.id833[.]ga

**Table 1: Domain hosting the credential phishing page**

Using PassiveTotal, we examined the historic DNS resolution data for this domain name. The results revealed that at the time of these phishing attempts, the domain **id833[.]ga** resolved to IP address **89.40.181[.]119** – the same Romanian IP address used to access David Satter’s email account on October 7 (see **Part 1**, The Case of David Satter).

This evidence suggests that the Bellingcat contributor and David Satter were both targeted by the same spear phishing campaign; this linkage will be explored further in the next section.

## Tiny.cc Enumeration

In examining the Tiny.cc shortened URLs found within the spear phishing emails sent to David Satter, we became curious as to the structure of how such links were constructed.

Tiny.cc provides a shortening service which allows users to create succinct URLs that redirect to some defined, usually long, website address. By way of example, we created a Tiny.cc shortened URL which redirects to a recent Citizen Lab report:

<http://tiny.cc/bj87iy> -> <https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/>

In this example, the Tiny.cc shortcode would be **bj87iy**. In the Tiny.cc application back-end database, this hash uniquely resolves to the target address of:

<https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/>

After conducting tests, we determined that these shortcodes are assigned in a sequential manner. For example, using the Tiny.cc API call for creating a shortened URL, we programmatically generated 8 links with a one-second delay between each call. The resulting shortcodes generated (in order) were as follows:

63q6iy  
73q6iy  
93q6iy  
e4q6iy  
p4q6iy  
r4q6iy  
t4q6iy  
24q6iy

After conducting numerous similar tests, we determined that shortcodes constructed within small temporal windows would be lexically close in the sense of the following 'base36 alphabet' sequence:

a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z,0,1,2,3,4,5,6,7,8,9

Successive shortcodes are constructed by iterating the leftmost character through this base36 alphabet. Once all 36 characters have been exhausted, this leftmost character reverts to the initial value of 'a', with the second character then iterating one position according to the same alphabet. This iterative process continues for each position of the shortcode (see Figure 22), enabling us to consider the shortcodes as a sort of base36 'counter'.

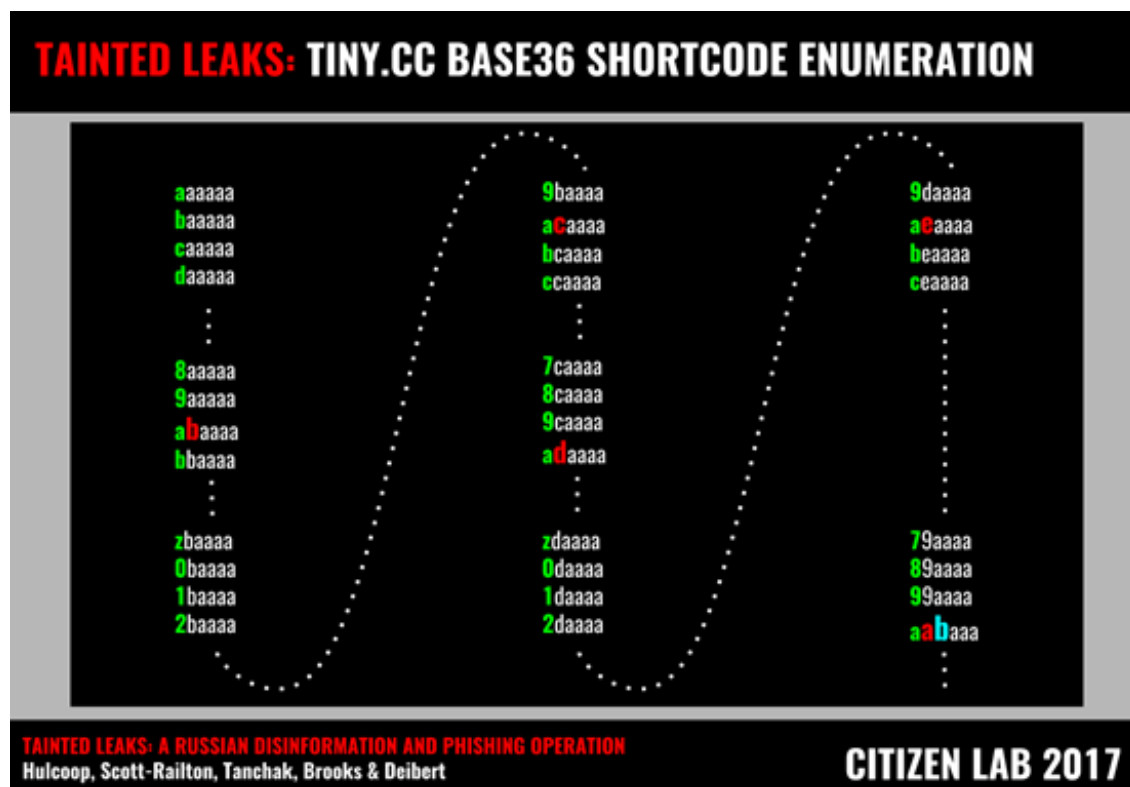


Figure 22: Enumerating the base36 shortcodes used by tiny.cc

Given this understanding of the shortcode design, we can measure the notional 'distance' between any pair of shortcodes. For example, the distance between the shortcodes **bj87iy** and **cj87iy** would be 1, and the distance between **bj87iy** and **bk87iy** would be 36.

This distance measurement gives an idea of how close two shortcodes are, and thus by extension, how close in time they were generated. We will revisit this notion of distance below.

Using this design knowledge, we considered the Tiny.cc shortcodes found in the October 5 and 7 phishing emails sent to David Satter. Using these as a starting point, we enumerated approximately 4000 adjacent shortcodes for each, and then examined the target web addresses to which these short links redirected. From this large list, we extracted all of the associated destination links (see Figure 23) which redirected to the malicious phishing domain described above in Table 1.

Tiny.cc URL	Destination	Ultimate Destination Phishing Page
<a href="https://tiny.cc/al">https://tiny.cc/al</a>	<a href="https://www.google.com/amp/tinyurl.com/z">https://www.google.com/amp/tinyurl.com/z</a>	<a href="http://myaccount.google.com-change-password-securitypagesettingmyaccountg">http://myaccount.google.com-change-password-securitypagesettingmyaccountg</a>
<a href="https://tiny.cc/jk">https://tiny.cc/jk</a>	<a href="https://www.google.com/amp/tinyurl.com/h">https://www.google.com/amp/tinyurl.com/h</a>	<a href="http://myaccount.google.com-change-password-securitypagesettingmyaccountg">http://myaccount.google.com-change-password-securitypagesettingmyaccountg</a>
<a href="https://tiny.cc/pl">https://tiny.cc/pl</a>	<a href="https://www.google.com/amp/tinyurl.com/h">https://www.google.com/amp/tinyurl.com/h</a>	<a href="http://myaccount.google.com-change-password-securitypagesettingmyaccountg">http://myaccount.google.com-change-password-securitypagesettingmyaccountg</a>
<a href="https://tiny.cc/fl">https://tiny.cc/fl</a>	<a href="https://www.google.com/amp/tinyurl.com/g">https://www.google.com/amp/tinyurl.com/g</a>	<a href="http://myaccount.google.com-change-password-securitypagesettingmyaccountg">http://myaccount.google.com-change-password-securitypagesettingmyaccountg</a>
<a href="https://tiny.cc/5l">https://tiny.cc/5l</a>	<a href="https://www.google.com/amp/tinyurl.com/j">https://www.google.com/amp/tinyurl.com/j</a>	<a href="http://myaccount.google.com-change-password-securitypagesettingmyaccountg">http://myaccount.google.com-change-password-securitypagesettingmyaccountg</a>
<a href="https://tiny.cc/ek">https://tiny.cc/ek</a>	<a href="https://www.google.com/amp/tinyurl.com/z">https://www.google.com/amp/tinyurl.com/z</a>	<a href="http://myaccount.google.com-change-password-securitypagesettingmyaccountg">http://myaccount.google.com-change-password-securitypagesettingmyaccountg</a>
<a href="https://tiny.cc/5l">https://tiny.cc/5l</a>	<a href="https://www.google.com/amp/tinyurl.com/h">https://www.google.com/amp/tinyurl.com/h</a>	<a href="http://myaccount.google.com-change-password-securitypagesettingmyaccountg">http://myaccount.google.com-change-password-securitypagesettingmyaccountg</a>
<a href="https://tiny.cc/yk">https://tiny.cc/yk</a>	<a href="https://www.google.com/amp/tinyurl.com/z">https://www.google.com/amp/tinyurl.com/z</a>	<a href="http://myaccount.google.com-change-password-securitypagesettingmyaccountg">http://myaccount.google.com-change-password-securitypagesettingmyaccountg</a>
<a href="https://tiny.cc/2l">https://tiny.cc/2l</a>	<a href="https://www.google.com/amp/tinyurl.com/z">https://www.google.com/amp/tinyurl.com/z</a>	<a href="http://myaccount.google.com-change-password-securitypagesettingmyaccountg">http://myaccount.google.com-change-password-securitypagesettingmyaccountg</a>
<a href="https://tiny.cc/zm">https://tiny.cc/zm</a>	<a href="https://www.google.com/amp/tinyurl.com/j">https://www.google.com/amp/tinyurl.com/j</a>	<a href="http://myaccount.google.com-change-password-securitypagesettingmyaccountg">http://myaccount.google.com-change-password-securitypagesettingmyaccountg</a>
<a href="https://tiny.cc/dj">https://tiny.cc/dj</a>	<a href="https://www.google.com/amp/tinyurl.com/j">https://www.google.com/amp/tinyurl.com/j</a>	<a href="http://myaccount.google.com-change-password-securitypagesettingmyaccountg">http://myaccount.google.com-change-password-securitypagesettingmyaccountg</a>
<a href="https://tiny.cc/im">https://tiny.cc/im</a>	<a href="https://www.google.com/amp/tinyurl.com/h">https://www.google.com/amp/tinyurl.com/h</a>	<a href="http://myaccount.google.com-change-password-securitypagesettingmyaccountg">http://myaccount.google.com-change-password-securitypagesettingmyaccountg</a>
<a href="https://tiny.cc/0j">https://tiny.cc/0j</a>	<a href="https://www.google.com/amp/tinyurl.com/j">https://www.google.com/amp/tinyurl.com/j</a>	<a href="http://myaccount.google.com-change-password-securitypagesettingmyaccountg">http://myaccount.google.com-change-password-securitypagesettingmyaccountg</a>
<a href="https://tiny.cc/im">https://tiny.cc/im</a>	<a href="https://www.google.com/amp/tinyurl.com/j">https://www.google.com/amp/tinyurl.com/j</a>	<a href="http://myaccount.google.com-change-password-securitypagesettingmyaccountg">http://myaccount.google.com-change-password-securitypagesettingmyaccountg</a>
<a href="https://tiny.cc/tj">https://tiny.cc/tj</a>	<a href="https://www.google.com/amp/tinyurl.com/z">https://www.google.com/amp/tinyurl.com/z</a>	<a href="http://myaccount.google.com-change-password-securitypagesettingmyaccountg">http://myaccount.google.com-change-password-securitypagesettingmyaccountg</a>
<a href="https://tiny.cc/8j">https://tiny.cc/8j</a>	<a href="https://www.google.com/amp/tinyurl.com/z">https://www.google.com/amp/tinyurl.com/z</a>	<a href="http://myaccount.google.com-change-password-securitypagesettingmyaccountg">http://myaccount.google.com-change-password-securitypagesettingmyaccountg</a>
<a href="https://tiny.cc/kj">https://tiny.cc/kj</a>	<a href="https://www.google.com/amp/tinyurl.com/h">https://www.google.com/amp/tinyurl.com/h</a>	<a href="http://myaccount.google.com-change-password-securitypagesettingmyaccountg">http://myaccount.google.com-change-password-securitypagesettingmyaccountg</a>
<a href="https://tiny.cc/0j">https://tiny.cc/0j</a>	<a href="https://www.google.com/amp/tinyurl.com/h">https://www.google.com/amp/tinyurl.com/h</a>	<a href="http://myaccount.google.com-change-password-securitypagesettingmyaccountg">http://myaccount.google.com-change-password-securitypagesettingmyaccountg</a>
<a href="https://tiny.cc/4j">https://tiny.cc/4j</a>	<a href="https://www.google.com/amp/tinyurl.com/z">https://www.google.com/amp/tinyurl.com/z</a>	<a href="http://myaccount.google.com-change-password-securitypagesettingmyaccountg">http://myaccount.google.com-change-password-securitypagesettingmyaccountg</a>
<a href="https://tiny.cc/5j">https://tiny.cc/5j</a>	<a href="https://www.google.com/amp/tinyurl.com/j">https://www.google.com/amp/tinyurl.com/j</a>	<a href="http://myaccount.google.com-change-password-securitypagesettingmyaccountg">http://myaccount.google.com-change-password-securitypagesettingmyaccountg</a>
<a href="https://tiny.cc/wj">https://tiny.cc/wj</a>	<a href="https://www.google.com/amp/tinyurl.com/j">https://www.google.com/amp/tinyurl.com/j</a>	<a href="http://myaccount.google.com-change-password-securitypagesettingmyaccountg">http://myaccount.google.com-change-password-securitypagesettingmyaccountg</a>
<a href="https://tiny.cc/oi">https://tiny.cc/oi</a>	<a href="https://www.google.com/amp/tinyurl.com/z">https://www.google.com/amp/tinyurl.com/z</a>	<a href="http://myaccount.google.com-change-password-securitypagesettingmyaccountg">http://myaccount.google.com-change-password-securitypagesettingmyaccountg</a>

**Figure 23: Some of the phishing links discovered during enumeration of the Tiny.cc shortcodes**

This enumeration led us to discover evidence suggesting that David Satter and the unnamed Bellingcat journalist were but two targets of a much larger credential phishing campaign. Notably, as mentioned above in **Part 1: A Second Phishing E-mail**, when we checked the particular Tiny.cc shortcode received by Satter, the unshortened link to the phishing page had been replaced with a benign URL: myaccount.google[.]com.

We were unable to conclusively determine the reason for this substitution. One theory suggests that the campaign operators mistakenly shortened incorrect destination URLs, while another posits that once the operators had successfully compromised a target’s account, they would inoculate the Tiny.cc link provided in the phishing email. Indeed, in the same batch of enumerated shortcodes from the October campaign, we found four additional shortcodes which also pointed to myaccount.google[.]com.

## Decoding the targets

We examined the “unshortened” URLs of shortcodes that were adjacent to the one sent to Satter, and discovered 25 distinct destination addresses of the form:

[https://www.google.com/amp/tinyurl.com/\(redacted\)](https://www.google.com/amp/tinyurl.com/(redacted))

These addresses were redirects which leveraged the previously mentioned, Google-hosted, open redirect page (google.com/amp/) to send a user to a link on the TinyURL.com shortening service. In every case, these TinyURL.com links were each designed to send their intended

victims to a tailored version of the following, fake, Gmail login page:

hxxp://myaccount.google.com-changepassword-securitypagesettingmyaccountgooglepagelogin.id833[.]ga/security/signinoptions/password

This domain, discussed above and noted in Table 1, at the time the phishing emails were sent, resolved to the Romanian IP address used to access Satter's Gmail account (see Part 1).

In order to bolster the social engineering aspect of these fake Gmail login pages, the operator used a series of base64-encoded URL parameter values in order to display the target's email address, and in some cases the target's name and Google profile image, into the appropriate fields on the fake login page.

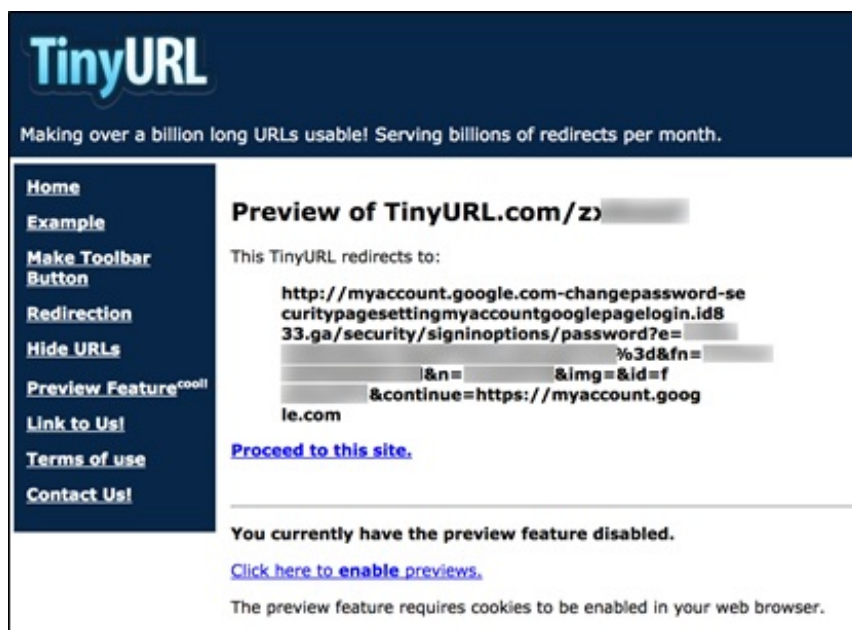


Figure 24: TinyURL preview of a second level redirect of a phishing link

The following example URL illustrates the use of these parameters (Figure 25):

```
http://myaccount.google.com-change-password-security-pagesettingmyaccountgooglepagelogin.id833[.]ga/security/signinoptions/password?e=<email_address>&fn=<full_name>&n=<first_name>&img=<link to google+ profile avatar>&id=<redacted>&continue=https://myaccount.google.com
```

Parameter	Holds Base64 Encoded Value of
e	Target email address
fn	Target full name
n	Target first name
img	Link location of target's Google Avatar

**Figure 25: URL parameter decoding from a phishing link**

By virtue of this pattern of URL parameters, we were able to determine the precise target of each of the phishing links we discovered during our enumeration process. The significance of this pattern of URL parameters will be revisited below in **Part 3**.

## Digging Deeper

Extending the search for suspicious URLs by fully enumerating the entire six-character shortcode sequence space in the above manner proved to be intractable.<sup>5</sup> However, the same ThreatConnect report discussed above also documented a previous APT28-attributed phishing attempt against Bellingcat journalist Aric Toler. On June 16, 2016, Toler was sent a strikingly similar Google-themed phishing email containing a Tiny.cc shortcode. Following the same process outlined above, we enumerated the shortcodes adjacent to the one published by ThreatConnect.

In doing so, we discovered another group of targets – **198 target email addresses in total**. In this earlier campaign, the unshortened URLs pointed directly to the likely phishing page (Figure 26):

```
http://mail-google-login.blogspot.com/p/google.html?e=<redacted>&fn=<redacted>&n=<redacted>&img=<redacted>&id=<redacted>&continue=https://myaccount.google.com
```

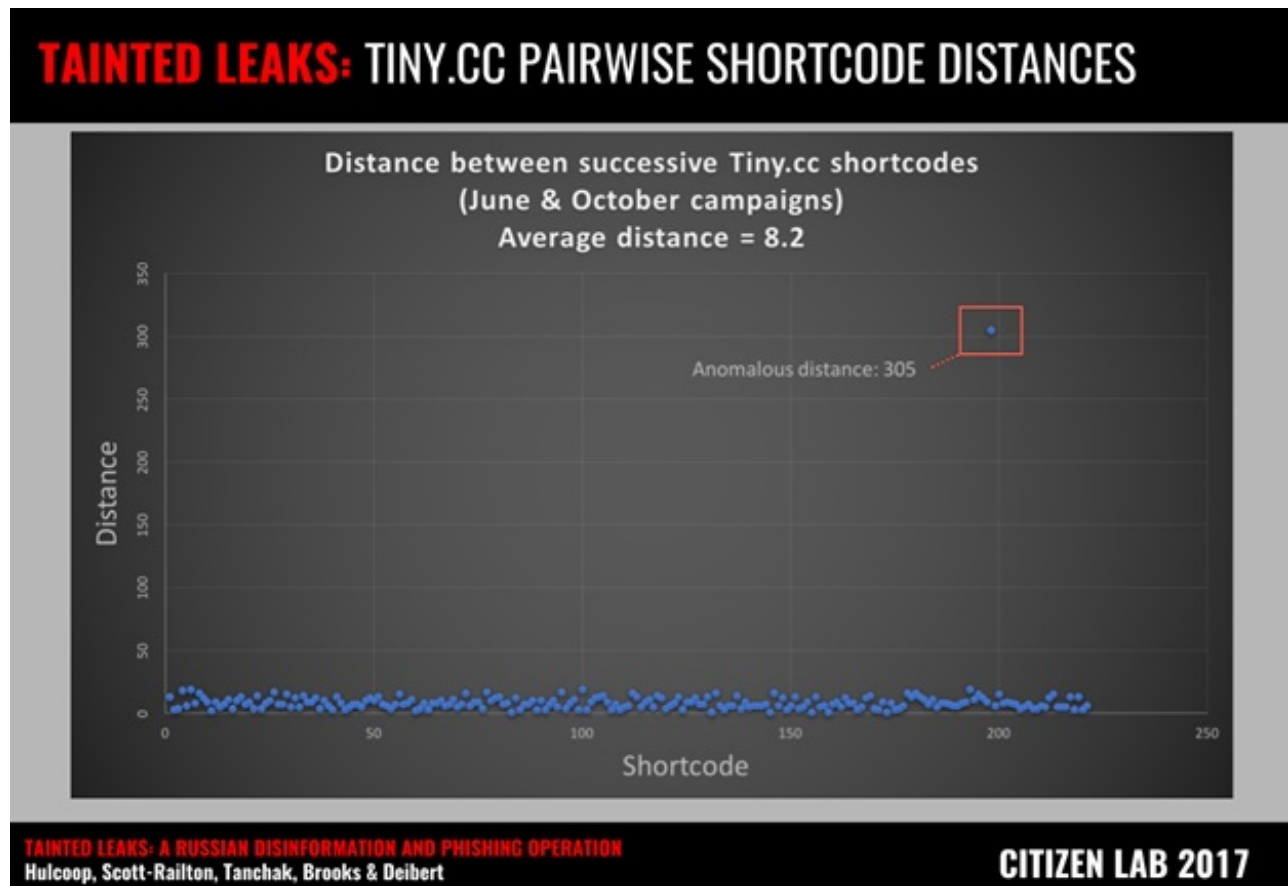
**Figure 26: URL parameters in June campaign against Aric Toler**

Notably, these links appear to be hosted on the Google Blogger service, and while these pages were already taken offline when we attempted to examine them, the same characteristic URL parameterization can be observed.

A brief analysis of the target list associated with these two campaigns is provided above (see [Pandora's Un-Shortening: Civil Society Targets Emerge](#)).

## Testing the Lure


We measured the distance between successive malicious Tiny.cc shortcodes seen in the June and October campaigns (Figure 27). In doing so, we observed fairly consistent distances between the shortcodes, perhaps indicating that the operators were generating these links via an automated process. However, one shortcode stood out, and we suspected this may have been a manual operator test.



**Figure 27: The anomalous distance of 305 immediately stood out from the average of 8.2, drawing our attention to the shortened link**

According to the parameters obtained from the phishing URL associated with this anomalous shortcode, we were able to decode the Gmail account targeted with this phishing link:



Parameter	Result after decoding
Email Address	myprimaryreger[@]gmail.com
Full Name	Åhlén خسروي
Google+ Profile Picture	

**Table 2: URL parameter values decoded**

This Google account, *myprimaryreger[@]gmail.com*, was also used in the registration of at least one other domain name which was linked in [prior research](#) to known or suspected APT28 activity. Such connections, while circumstantial, further support the link to Russia-based threat actors.

In [Appendix B](#) we provide a brief description of why we think the account is being used by the operator, and how the account uses Google Plus posts to embed images into phishing e-mails.

## Part 3: Connections to Publicly Reported Operations

*This section outlines the connections and overlaps between the operation described in this report and other, publicly-reported Russian-affiliated cyber espionage campaigns.*

The operator test uncovered during our enumeration of the Tiny.cc shortcodes (see [Testing the Lure](#) above), provides a circumstantial link to APT28, however there are other potential links. In this section, we outline other comparisons between this campaign and other publicly reported operations that have a Russian nexus. We identify marked similarities to a collection of phishing links now attributed to one of the most publicly visible information operations in recent history: the targeting of the 2016 US Presidential Campaign.

### A Bit More Abuse

The phishing URLs in this campaign were encoded with a distinct set of parameters using base64. When clicked, the links provided key information about the targets to the phishing website. An identical approach to parameters and encoding (see Figure 28 below) has been seen before: in the March 2016 phishing campaign that targeted Hillary Clinton's presidential campaign and the Democratic National Committee. This similarity suggests possible code re-use: the two operations may be using the same phishing 'kit'.

The [campaign](#) that targeted the DNC also included the same Google security-themed phishing ruse, and abused another URL shortening service, [Bit.ly](#). In June 2016 Dell SecureWorks published a [report](#) attributing the operation to APT28, a threat actor [routinely associated with](#)



bypass the security of two-factor authentication.

Domain linked to this campaign:

**myaccount.google.com-changepassword-securitypagesettingmyaccountgooglepage**login.id833[.]ga

Domain mentioned by Mandiant, linked to APT28:**myaccount.google.com-changepassword-securitypagesettingmyaccountgooglepage**.id4242[.]ga

The similarities in naming and subdomain structure are immediately apparent. The two domains (**id833[.]ga** and **id4242[.]ga**) also share a common name server. However, we were not able to find specific registration overlaps between the domains or servers.

Furthermore, during the campaign period, the domain identified by Mandiant, **id4242[.]ga** resolved to **89.32.40[.]238**. This IP also resolves to a range of other suspicious domains with highly similar naming schemas to those connected to the infrastructure used against Satter. The link used to phish John Podesta, as depicted above, also shares distinct naming and subdomain similarities with domains linked to the phishing operation against Satter (see Figure 28):

Domain targeting Podesta, linked to APT28: **hxxp://myaccount.google.com-securitysettingpage[.]tk**

During the campaign in March 2016, this domain was hosted at IP address **80.255.12[.]237**

Publications from numerous private industry groups attribute **89.32.40[.]238** and **80.255.12[.]237** (as well as related domains) to APT28. While we are able to point out that there are significant commonalities in domain naming and subdomain structure between the campaign targeting Satter and domains linked to these IPs, we are not able to make a more conclusive technical link to APT28.

While industry groups as well as the U.S. government have publicly connected APT28 with Russian state actors, we are not able to use infrastructure analysis alone to conclusively connect the operation against Satter to a particular state sponsor. Connecting this infrastructure to a specific government would require additional evidence which is not, to our knowledge, available in the public domain.

## The Challenge of Attribution

---

While the order of events surrounding the phishing, credential theft, and eventual leak of tainted documents belonging to David Satter would seem to point to CyberBerkut, the characteristics of Russian information operations make the task of attribution to a state sponsor challenging. As a consequence, there is no “smoking gun” connecting the evidence we have assembled to a particular Russian government agency, despite the overlaps between our evidence and that presented by numerous industry and government reports concerning Russian-affiliated threat actors.

Addressing the topic of attribution requires nuance and appreciation of the unique character of

Russian cyber espionage: its deliberate cultivation of organized criminal groups as proxy operators, and the high number of independently operating, overlapping, and sometimes competing spy agencies and security services all of whom work within a broad culture of barely concealed corruption. As one study on Russia notes, Russia's many security agencies "are granted considerable latitude in their methods, unconstrained by the concerns of diplomats or the scrutiny of legislators."

Russia's approach to the use of proxy actors in the criminal underworld in particular is informed by a very elaborate strategy around information operations and control. Although this strategy has roots that go back deep into Soviet (and even earlier Russian) history, it was more fully elaborated as a component of hybrid warfare, also known as the Gerasimov doctrine or "non-linear warfare," and infused with deeper resources after the 'color revolutions,' the 2011 Moscow protests, and upon reflection of the events of the Arab Spring. The overall Russian approach has been described as a form of "guerrilla geopolitics" in which "a would-be great power, aware that its ambitions outstrip its military resources, seeks to leverage the methodologies of an insurgent to maximise its capabilities." Cultivating organized criminal groups is a fundamental component of this approach, as evidenced in the annexation of Crimea which was undertaken in coordination with criminal elements who provided "political and military muscle." Russian security officers are also known to routinely dabble in the proceeds of underworld criminal operations for illicit revenue of their own, and as a result can even prioritize criminal over national security concerns.

In the digital arena, this doctrine is manifest in the cultivation of Internet-focused organized criminal groups who operate partially on behalf of or in support of the Putin regime, and partially oriented around their own pecuniary gain in online financial fraud and other schemes. There is evidence Russian hackers are being given wide latitude to undertake criminal activities as long as it conforms to Russian security agencies' wishes. Multiple Russian-affiliated operators could compromise the same target unwittingly and without seeming coordination. This "piling on" around a target further complicates attribution. This complex proxy strategy, as well as the multiple, competing agencies behind the proxies, is often lost or overlooked when companies and government agencies jump quickly to attribution around Russian cyber espionage.

While it is possible that a proxy actor is implementing the front-end collection component of the phishing campaign we are describing, the scale of the targeting also suggests a well-resourced actor, such as a nation state. The thread linking all of the targets is their connection to issues that the Russian government cares about. The targets are people whose positions or activities give them access to, or influence over, sensitive information of specific interest to Russia. This links an otherwise extremely diverse target set, which ranges from domestic Kremlin critics and journalists, to anti-corruption investigators, foreign government personnel, and businesspeople.

The data collected from such a campaign would come in more than a dozen languages, and concern a diverse range of political, military, and policy issues from at least 39 countries and 28 governments. In addition, such a campaign would be likely to generate large volumes of

data. For this reason, a professionalized, well-resourced operator would be needed for any effective post-collection analysis of the stolen data. Even greater resources would be required to analyse, and in some instances carefully modify in a short timeframe, the contents of stolen email and cloud-storage accounts for the purposes of seeding disinformation via *tainted leaks*.

The diversity and presumed cost of analyzing the stolen data along with the clear Russian nexus for the targets is only circumstantial evidence of a Russian connection. It should be evaluated in the context of the other pieces of circumstantial evidence we present, including the overlaps in tactics with known Russia-linked actors, and the prominent role of CyberBerkut.

## Part 4: Discussion

---

*In this section, we examine the troubling relationship between espionage and disinformation, particularly in its latest digital manifestation, and elaborate on how civil society is particularly at risk from such new tactics.*

### Tainted Leaks: A New Trend

---

The recent theft and disclosure of documents (branded as a “leak”) from the presidential campaign of Emmanuel Macron is the highest profile case in which it appears that falsified documents were inserted amongst real, stolen documents. The documents falsely implied a range of improper or questionable activities. The false stories implied by these documents were then highlighted in campaigns promoted with twitter bots and other techniques. The leak-branded release had followed the release, several days earlier, of a quickly-debunked story, supported by falsified documents, alleging that Macron held foreign bank accounts.

In the case of the leak-branded releases during the 2016 US presidential election, the publicly-available evidence connecting these releases with Russian-affiliated cyber operations is largely circumstantial, but compelling. It is reported, and highly probable, that stronger evidence is available in classified venues. Building on initial reports by Trend Micro that the Macron campaign was targeted by APT28, follow-up reports have pointed to Russian involvement in the breach, and the tainted leaks.

The Macron case continues to develop, and many elements are still uncertain, including whether the Macron campaign was deliberately seeding their own communications with false documents, intended to slow down operators’ analysis pipeline. However, it is not the first case in which evidence or claims of tainted leaks have surfaced.

Documents stolen from the Open Society Foundations, which had been the victim of a breach, were modified and then released in a tainted leak by CyberBerkut in a post dated November 21 2015. The tainting included careful alterations, such as modifying budget documents, to make it appear that certain Russian civil society groups were receiving foreign funding. The case became publicly visible because elements of the same stolen set were re-released on the leak-branded website “DC Leaks,” without the tainting.

In the case of David Satter, whose personal email accounts had similarly been breached, and then tainted, materials were **edited, spliced, and deleted, while new text was added.**

**Fiction was added to fact to create a hybrid “tainted leak.”** The tainted leak told a series of new, false stories, intended not only to discredit Satter, but to support domestic narratives familiar to many Russians: of foreign interference, and of a foreign hand behind criticism of the government.

## Falsehoods in a Forest of Facts

---

Recent leaks by genuine whistleblowers, as well as “leak”-branded releases of materials stolen by cyber espionage operations (e.g. “DC Leaks” or “Macron Leaks”) are appealing because they appear to provide an un-filtered peek at people speaking privately. Like an intercepted conversation, they feel closer to the “truth,” and may indeed reveal unscripted truths about people and institutions. It is hard not to be curious about what salacious details might be contained within them. In the 2016 United States presidential election, it was evident that the release, although clearly intended to influence the election, was viewed by most media organizations as having intrinsic newsworthiness, and thus the contents of leaks were often quickly amplified and repeated.

The potential of leaks to attract attention makes large dumps of stolen materials fertile ground for tainting. A carefully constructed tainted leak included in a set of real stolen material is surrounded by documents that, by juxtaposition, indirectly signal that it is legitimate. This could help the tainted leak survive initial scrutiny by reporters and others seeking corroboration. Coupled with a media strategy, or social-media amplification campaign that selectively highlights the fake or the narrative that the fake supports, leak tainting poses a serious problem to both the victim of the breach, and whoever is implicated by the disinformation.

The spread of disinformation can contribute to cynicism about the media and institutions at large as being untrustworthy and unreliable, and can cultivate a fatigue among the population about deciphering what is true or not. By propagating falsehoods, the aim is not necessarily to convince a population that the falsehood is true (although that outcome is desirable) but rather to have them question the integrity of all media as equally unreliable, and in doing so “foster a kind of policy paralysis.”

## Tainted Leaks Place a Unique Burden on Breach Victims

---

Should a tainted document gain traction, there is a burden on the victim of the disinformation to prove that the leaks are not genuine. This challenge may be difficult. Victims of breaches may be unable, unwilling, or forbidden to release original documents. Moreover, they may not wish to be drawn into fact-checking their own stolen data. This problem is likely to be especially true if the operators behind the tainted leaks have chosen documents that are themselves sensitive.

A Russian anti-corruption activist whose name has been seeded into such sensitive reports may not be able to convince the original victim of the breach to release the authentic document. Indeed, such a person may not even be able to determine exactly which parts of



the document are real, and which are fake, beyond what they know to be true about themselves.

Meanwhile, members of the public do not have the ability to carefully verify the integrity of such dumps, either as a whole, or specific documents within them. Indeed, even journalists reporting on accusations or falsehoods may be unable to obtain explicit confirmation of which exact material has been faked. If a tainted document is carefully constructed from real, verifiable elements, it may be especially difficult to identify as a fake. Even if journalists do the hard digging and analysis, they may not be able to publish their results in a timely enough fashion to matter. By the time their work is complete, the false information may have embedded itself into the collective consciousness.

Disinformation can persist and spread unless concerted measures are taken to counter it.

Even more insidious is the fact that studies have found that attempts “to quash rumors through direct refutation may facilitate their diffusion by increasing fluency.” In other words, efforts to correct falsehoods can ironically contribute to their further propagation and even acceptance.

Not all tainted leaks work as intended to cause maximum harm. Almost immediately following the “Macron Leaks,” the Macron campaign responded quickly, and stated that the “leaks” included fakes. In the fast-moving media environment in the days before voting, this move may have led to uncertainty about the factual nature of the release in the minds of many journalists, dimming enthusiasm to quickly report ‘finds.’ Amplification of the “leaks” was further blocked by a “recommendation to media” by the French electoral authority to not “relay” the leaks. The authority pointed to the presence of fakes, and warned of possible legal implications for reporting the story.

Following the voting, staff from the Macron campaign claimed in the media that the stolen documents also likely contained fakes created by the campaign, designed to waste the time of intruders. This claim also cast further doubt on the veracity of any documents contained in the “leaks.”

## Tainted Leaks: Old Methods, New Tactics

---

Stealing digital information for intelligence purposes is a well-known and commonly practiced tactic used by states. However, a unique aspect of Russian cyber espionage distinguishing it from other governments is the public release of exfiltrated data intended to embarrass or discredit adversaries. Known as “kompromat”, this type of activity is common in Russia, and was previously used by the Soviet Union, and is evident in the publication of emails on Wikileaks related to United States officials involved in the 2016 U.S. presidential election campaign.

Releasing Satter’s e-mails could be roughly described as kompromat. However, with his cooperation we were able to identify a second feature of the release: the deliberate tampering with the content of his messages. This mixing of fact and falsehood is thus also a disinformation strategy.

In Russian / Soviet military doctrine, the practice of deliberately propagating forged documents and disinformation is known as “dezinformatsiya”, referring to manipulation of information in the service of the propagation of falsehoods. Although practiced for decades by Russia and the Soviet Union, the use of *dezinformatsiya* in connection with cyber espionage is a new and troublesome frontier in structured digital disinformation.

## Why Target Civil Society?

---

Our investigation identified civil society targets inside and outside of Russia. This targeting is consistent with a general consensus on how the Russian regime thinks: whether domestic or foreign, civil society is treated as a threat to the regime, its extended kleptocracy, and the sovereignty of the country.

There are at least two reasons why civil society factors highly into Russian perceptions of threats. First, independent civil society groups can create difficulties for the regime by spotlighting corruption and abuse of power, speaking freely about issues the government would rather keep in the shadows, and mobilizing people into organized opposition.

Those unfamiliar with the Russian experience may overlook a second motivation, which is drawn from the larger Russian narrative of humiliation and defeat at the hands of the United States and its allies at the end of the Cold War. Some Russian leaders, especially those tied to the old Soviet system, resent US triumphalism, and see local civil society (except for those under their direct control) as instruments of US and western interference in Russian domestic politics. For example, Putin used the term “active measures” to describe the actions of then-Secretary of State Hillary Clinton during the 2011 Moscow demonstration. This narrative of Russia as a “besieged fortress” is used as justification for the repression and targeting of civil society groups both inside Russia proper, in the former Soviet spaces, and abroad.

While often overlooked by western media and policymakers, this threat model translates in practice into targeted digital surveillance operations on civil society, both domestically and abroad. Of special concern to the government are NGOs, journalists, and activists that are seen as having links to the West and / or are funded by western governments. Many of the targets of this campaign are connected in some degree to United States-based think tanks and fellowships.

Of equal concern to the government, however, are the actions of domestic NGOs and individuals. As our report shows, a principal motivation for the targeting of David Satter and the tainting of leaks derived from materials stolen from him was to falsely portray local Russian groups as having affiliations and even funding ties to western organizations and the U.S. government.

## Conclusion

---

Tainted leaks are a growing and particularly troublesome addition to disinformation tactics, and in the current digital environment are likely to become more prevalent. In the 2017 French

presidential election, tainted leaks appear to have been used in an attempt to discredit the political party and candidate for election directly. The target of the tainting was roughly the same entity that suffered the breach. In the cases we analyzed, however, tainted leaks were used to discredit third parties who had not been the victims of the original breach. This difference highlights yet another facet of the growing trend of leak-branded releases, and the challenges they pose.

Tainted leaks—fakes in a forest of facts—test the limits of how media, citizen journalism, and social media users handle fact checking, and the amplification of enticing, but questionable information. As a tactic, tainted leaks are an evolution of much older strategies for disinformation, and like these earlier strategies, pose a clear threat to public trust in the integrity of information. Interestingly, while the tainting we describe appears to have a primarily domestic aim, to discredit elements of the Russian opposition, it is readily applied globally.

The report identified a phishing campaign with over 200 unique targets from 39 countries. We do not conclusively attribute the technical elements of this campaign to a particular sponsor, but there are numerous elements in common between the campaign we analyzed and that which has been publicly reported by industry groups as belonging to threat actors affiliated with Russia.

Given Russia's well-known preference for the use of proxy actors, it would be highly unlikely that a group such as ours, which relies on open source information, would be able to discover a conclusive link in a case like this. However, it is worth reiterating that the resources of a government would likely be necessary to manage such a large and ambitious campaign, given the number of languages spoken by targets, and their areas of work. The group includes a former Russian Prime Minister, a global list of government ministers, ambassadors, military and government personnel, CEOs of oil companies, and members of civil society from more than three dozen countries.

The targets we found are connected to, or have access to, information concerning issues in which the Russian government has a demonstrated interest. These issues range from investigations of individuals close to the Russian president, to the Ukraine, NATO, foreign think tanks working on Russia and the Crimea, grantmakers supporting human rights and free expression in Russia, and the energy sector in the Caucasus.

Considering this primary Russian focus, as well as the technical evidence pointing to overlaps and stylistic similarities with groups attributed to the Russian government, we believe there is strong circumstantial—but not conclusive—evidence for Russian government sponsorship of the phishing campaign, and the tainted leaks.

The civil society targets of this operation deserve special attention. At least 21% of the targets from our set were journalists, activists, scholars and other members of civil society. All too often, threats against civil society groups receive second-billing in industry reporting and media coverage of government-linked operations.

Yet, in this case, members of civil society were both the targets of disinformation in the form of

tainted leaks, and represented a large proportion of the phished targets. In a cautionary note for grantmakers, several dozen targets all held the same fellowship, from the same organization. This common affiliation suggests that they may have been targeted because of their relationship with the grantmaker.

We hope this report will encourage others to engage in further research into the techniques used to propagate tainted leaks, as well as serving as a reminder of the often under-reported presence of civil society targets among government-linked phishing and malware operations.

## Acknowledgements

---

Special thanks to David Satter, Raphael Satter, and the Open Society Foundations for cooperating and providing us with materials necessary to conduct the investigation.

Thanks to the Citizen Lab team who provided review and assistance, especially Bill Marczak, Masashi Crete-Nishihata, Etienne Maynier, Adam Senft, Irene Poetranto, and Amitpal Singh.

We would like to thank additional researchers for comments and feedback including Jen Weedon, Alberto Fittarelli, Exigent Petrel and TNG.

Support for Citizen Lab's research on targeted threats comes from the John D. and Catherine T. MacArthur Foundation, the Open Society Foundations, the Oak Foundation, Sigrid Rausing Trust, and the Ford Foundation.

## Appendix A: The Tainting

---

This document compares an original document stolen from journalist David Satter with a tainted leak released by CyberBerkut.

Legend:

Black = original, unchanged

Blue = added text in the tainted leak

Red = removed text in the tainted leak

~~The Radio Liberty~~ Russian investigative reporting project is gaining traction and producing significant journalism ~~for the site of the Radio Liberty Russian Service~~. In this way, it is making a contribution to Western efforts to provide the Russian population with objective information.

In the first ~~nine~~ **ten** months of 2016, ~~fourteen~~ **twenty four** investigative or in depth articles have been published under aegis of the project. In addition, six other articles are in progress or are awaiting publication. The following is a list of the articles that were published as of ~~September 30~~ **October 20**, 2016:

1. Vladimir Voronov, "Import Replacement for Rogozin," January, 2016 [mismanagement in the defense industry] ([RFE/RL](#))
2. Eldar Gus'kov, "The Empire and Prison of Gaydamak," February, 2016 [the life and fate of an arms trader] ([RFE/RL](#))
3. Vladimir Voronov, "Kosmos A la Russe," March 3, 2016 [the state of Russian space program] ([RFE/RL](#))
4. **Elizaveta Surnachyova, "Informational Stuffing: What is Known about Each President Sergei Roldugin," March 29, 2016 [an investigation on a Putin close friend] (RBC)**
5. **Vyacheslav Kozlov and Ivan Tkachyov, "The Budget of Katherine Tikhonova's Fund Has Grown by Half," April 6, 2016 [the fund of Putin's daughter] (RBC)**
6. Alexander Podrabinek, "Degree of Risk," April 11, 2016 [the fate of today's opposition compared to the experience of Soviet dissidents] ([RFE/RL](#))
7. Sergei Dibrov, "Vie Moved Toward the Tragedy for Several Months," May 2, 2016
8. Sergei Dibrov, "A Black Day in the History of Odessa," May 2, 2016 [two part series on the Odessa trade union building fire] ([RFE/RL](#))

9. Vladimir Voronov, "'Ros Vacuum Cleaner' Sergei Chemezov," May 8, 2016 [the corruption of a Putin favorite] ([RFE/RL](#))

10. Galina Sidorova, "Under the 'Roof' of the Foreign Ministry," May 15, 2016 [how the foreign ministry abandoned its principles] ([RFE/RL](#))

11. Ela Znamenskaya, "Stuffed, Bought, Beat, Pushed Aside," June 19, 2016 [how elections are falsified] ([RFE/RL](#))

12. Mark Galeotti and Anna Artutunyan, "The Hybrid Business of the Kremlin," June 24, 2016 [the state's takeover of business] ([RFE/RL](#))

**13. Alexei Navalny, "Igor Shuvalov's Tsar-apartment Costs 600 Times as Ordinary Apartments He Laughed at," July 4, 2016 [the corruption of Putin's close friend] (Anti-Corruption Foundation)**

14. Natalia Rostova, "How the Press Elected the President," July 8, 2016 [how the press helped Yeltsin steal the 1996 election] ([RFE/RL](#))

15. Ela Znamenskaya, "It's Necessary to Live. But How?" August 7, 2016 [the fate of the regional press] ([RFE/RL](#))

**16. "Portraying Benefactor: "Who Pays for the Projects Related to Putin," August 9, 2016 [the sponsoring of anti-democratic movements] (Slon)**

17. Vladimir Voronov, "Requiem for the Mi-28H," August 30, 2016 [chaos in military procurement] ([RFE/RL](#))

18. Evgeny Gusev, "The King of State Orders," September 5, 2016 [the corruption of Putin's friends, the Rotenberg brothers] ([RFE/RL](#))

**19. Irina Dolinina and Alesya Marokhovskaya, "Journalists Have Found Analogues of the Ozero Cooperative All Over the Central Russia," September 8, 2016 [corruption in the regions] (Slon)**

**20. Alexei Navalny, "There, Beyond the 6-Meter-High wall of Medvedev's Dacha," September 15, 2016 [an investigation on prime minister Medvedev] (Navalny.com)**

**21. Alexei Navalny, "He is Putin's Cook. He is Putin's Troll. He is a Billionaire," October 4, 2016 [the fate of Prigozhin, one of the businessmen close to Putin] (Navalny.com)**



22. Maria Zholobova and Maria Borzunova, “Apartment Worth More than Half a Billion Was Found at Putin's Ex-Bodyguard Samename,” October 9, 2016 [the corruption of Putin inner circle] (TV Dozhd)

23. Irina Gruzina, Ivan Vasiliev, Irina Skrynnik, “Samolet Development is Ready to IPO,” October 12, 2016 [about Moscow Oblast governor's illegal business ties] (Vedomosti)

24. Alexei Navalny, “How Katherine Tikhonova's Fund is Doing,” October 18, 2016 [the fund of Putin's daughter] (Navalny.com)

Of the **five six** articles that are in the “pipeline,” **three four** are finished and will soon be published. These are articles about the Russian modeling business by Eldar Gas'kov, the political ambitions of Russian nationalists by Mark Galeotti and Anna Arutunyan, and the crushing defeat of Russian arms in 1982 in the battle that took place between Israel and Syria in the Bekaa Valley of Lebanon. The articles that are still being written are a history of the Metropol Affair, the first attempt to resist censorship in the Soviet Union, by Galina Sidorova and an analysis of the structure of power and corruption in the Samara Oblast by Vladimir Voronov. **Besides, on October 24-25, Vedomosti columnist Elena Vinogradova will publish an article about Moscow Oblast issues in which senior Russian officials and businessmen close to Putin will be mentioned.**

Of the articles that have been published **on in** the Russian **site media**, four have been translated into English and published on the site of the Henry Jackson Society. These are the articles about Rogozin, Gaydamuk, Chemezov and Russian space exploration. **A backlog of articles to be translated has developed because Arch Tait, our translator, had to take a break to work on the translation of a book. He is now back at work and will begin translating some of the pieces.** Still to be worked out, however, are arrangements for publishing these pieces **in** English **on the English Language** site of Radio Liberty. David Satter will be traveling to Prague in late October during which time he hopes to resolve this matter with the newly appointed President of Radio Liberty! Radio Free Europe, Thomas Kent.

The media in Russia is severely censored. An illustration of this is the way in which it treated the new book by David Satter, “The Less You Know, the Better You Sleep: Russia’s Road to Terror and Dictatorship under Yeltsin and Putin,” which described the role of the Putin regime in acts of terror against the Russian population. The opposition web site, Kasparov.ru had devoted seven articles to the book. It summarized each of the book’s five chapters in separate articles and then published two articles about the excerpt from the book that was carried in the National Review. Radio Liberty published a large excerpt from the book and it was given extensive coverage by the Voice of America Russian Service and RTVi. The book, however, was not mentioned by a single media outlet in Russia, including those such as TV Dozhd and Ekho Moskvy that are praised for their independence.

Against this background, it is not an exaggeration to say that the articles being published

on the Radio Liberty [site](#), [Vedomosti](#) and [RBC](#) sites are a vital source of uncensored information. In this regard, it is worth calling particular attention to the two part series on the 2014 Odessa trade union building fire, the provocation that inspired a flood of Russian volunteers to fight in Ukraine and the definitive piece by Natalia Rostova on the unsavory role of the Russian press in the election of Yeltsin in 1996. These pieces provided truthful versions of historical events that cast a long shadow over the welfare of Russia today and are essential to be understood if Russia is to make progress.

In December, Russia will mark the 25th anniversary of the fall of the Soviet Union and in November of next year, the 10th anniversary of the Bolshevik Revolution. “We will be commissioning articles on a wide array of topics linked to these historical events, including the teaching of history in Russian schools, how the Soviet period is being understood by Russia’s leaders and what steps have been taken to commemorate the victims of Soviet era crimes. We will also seek to write about some modern day mysteries, including the death of oligarch Boris Berezovsky and the true story of who took part in the sniper massacre in Ukraine on February 20, 2014.

We are seeking to expand our network of journalists and have had some success despite the risks of writing ~~for Radio Liberty without the protection of a full-time job~~ [articles](#). This effort will continue.

**Figure 29: Full text of the tainted leak released by CyberBerkut showing tainting**

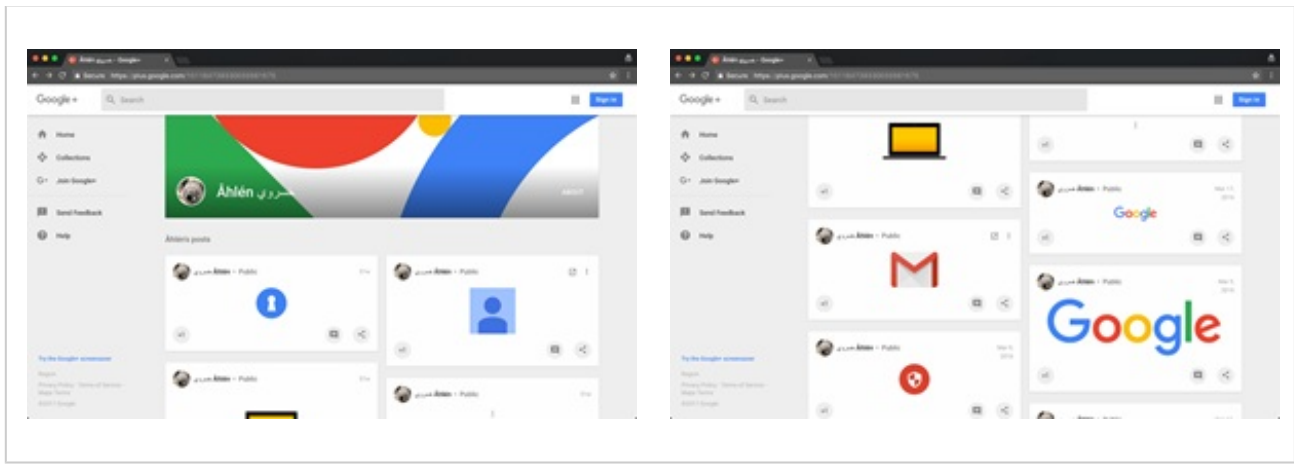
## Inserted Articles and their Contents

Article	Author	Theme
<a href="#">Informational Stuffing: What is Known about Each President Sergei Roldugin</a>	Elizaveta Surnachyova	Discusses the relationship between Putin and Sergei Roldugin (a cellist and financial associate of Putin). Roldugin is friends with many Putin insiders, and holds a 3.2% stake in Bank Rossiya. He also formerly ran two media groups and one oil company.
<a href="#">The Budget of Katherine Tikhonova’s Fund Has Grown by Half</a>	Vyacheslav Kozlov and Ivan Tkachyov	Innopraktika, a fund managed by Putin’s daughter, saw a very large funding increase.
<a href="#">Igor Shuvalov’s Tsar-apartment Costs 600 Times as Ordinary Apartments He Laughed at</a>	Alexei Navalny	Part of a series on the shell companies used by Igor Shuvalov, and his purchase of a lavish and extremely expensive apartment.
<a href="#">Portraying Benefactor: “Who Pays for the Projects Related to Putin</a>		Examines the processes by which oligarchs repay the Russian president by contributing money to “charities” and pet projects. These include the funds managed by Tikhonova and Roldugin.

Article	Author	Theme
<a href="#"><u>Journalists Have Found Analogues of the Ozero Cooperative All Over the Central Russia</u></a>	Slon	Relates to a Transparency International and Meduza.io investigation documenting replications of the Ozero Cooperative (Putin's dacha organization) across Russia. This cooperative involves private dacha (cottage) communities in which politicians, public servants and businessmen live in close proximity, allowing them to conduct informal meetings.
<a href="#"><u>There, Beyond the 6-Meter-High "fall of Medvedev's Dacha"</u></a>	Alexei Navalny	Discusses the 80 hectare (officially only 2 hectare) property belonging to Medvedev, and paid for by oligarchs through contributions made to "charitable funds."
<a href="#"><u>He is Putin's Cook. He is Putin's Troll. He is a Billionaire</u></a>	Alexei Navalny	A look at Dmitry Rogozin, who runs the "troll factory" on Savushkina Street in St. Petersburg. He also controls a series of unrelated companies providing everything from catering to cleaning services to power distribution which benefit from government contracts.
<a href="#"><u>Apartment Worth More than Half a Billion Was Found at Putin's Ex-Bodyguard Samename [sic]</u></a>	Maria Zholobova and Maria Borzunova	Putin's former bodyguard and now governor of Tula region, Alexei Dyumin, is registered as owning an apartment worth between 500-700 million rubles. Curiously, the apartment was purchased while Dyumin was serving in the Russian Ministry of Defence. .
<a href="#"><u>Samolet Development is Ready to IPO</u></a>	Irina Gruzinova, Ivan Vasiliev, Irina Skrynnik	"Samolet Developments" is a property development firm building condos. The company was purchased by Invest AG. Samolet Developments managed to develop land and obtain permits where others could not given its close ties to the governor of Moscow region, Andrey Vorobev. His brother, Maksim, is one of Samolet's founders.
<a href="#"><u>How Katherine Tikhonova's Fund is Doing</u></a>	Alexei Navalny	This report describes multi-million dollar contracts from state firms with the science and tech fund managed by Putin's daughter. The fund also received "anonymous donations" totalling roughly half its budget, leading to 2015 revenues of 877 million rubles. Includes quotes of vague and nonsensical project descriptions used to justify payouts.

## Appendix B: Test Account

Examining the Google+ page for the **myprimaryreger[.]gmail.com** account reveals a suspicious series of posts:



**Figure 30 B: Google+ profile page for myprimaryreger[.]gmail.com**

Each of the Google+ profile posts by this user contain images which are routinely observed in legitimate security warning emails sent by Google. Once an image file is uploaded to a Google+ profile post, it is copied to Google servers and can be obtained using an associated perma-link.

We suspect that the purpose of these posts is to allow the operator to embed links to Google-specific images into their phishing emails in the hopes that linking to images hosted *on Google servers* will somehow thwart Gmail malicious email detection controls.

## Appendix C: Indicators of Compromise

Domain Names	IP Addresses	Email Addresses
id833[.]ga	89.40.181.119	g.mail2017[.]yandex.com
id834[.]ga	89.32.40.238	annaablony[.]mail.com
id9954[.]gq	80.255.12.237	myprimaryreger[.]gmail.com
id4242[.]ga		
mail-google-login.blogspot[.]com		
com-securitysettingpage[.]tk		

## Footnotes

<sup>1</sup> “Colour Revolution” is a term that has been widely used to describe the pro-democracy protests and social movements that occurred in the early 2000s throughout the former Soviet Union.

<sup>2</sup> Several individuals were targeted in both of the two distinct campaigns we analysed.

<sup>3</sup> The Citizen Lab receives financial support for its research from a range of funders, including the Open Society Foundations. See <https://citizenlab.ca/about/>

<sup>4</sup> “Vedomosti” is a Russian language daily news service connected to The Moscow Times (and in which The Financial Times and Dow Jones had a stake until 2015, when Vedomosti and The Moscow Times were bought out by Russian business interests).

<sup>5</sup> The six character base36 sequence space contains over 2.1 billion combinations. Checking each one with a one-second delay (so as not to abuse the Tiny.cc web service) would take approximately 66 years.