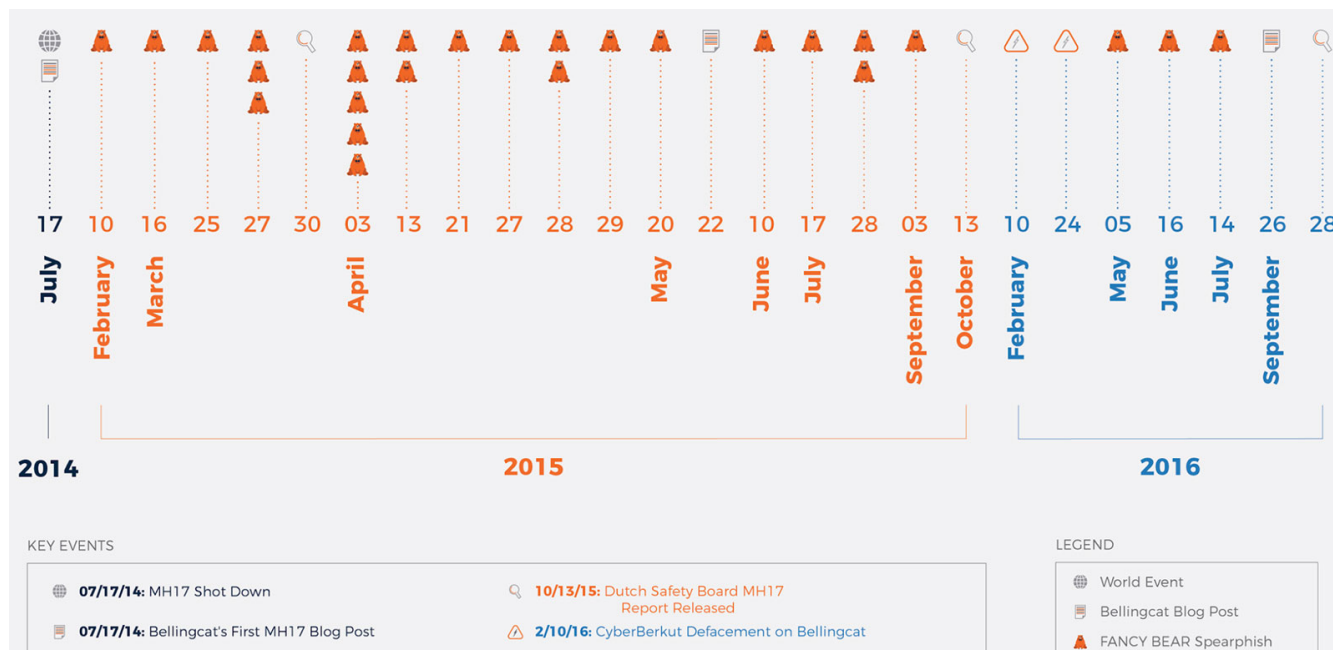


# Belling the BEAR



## ThreatConnect reviews activity targeting Bellingcat, a key contributor in the MH17 investigation.

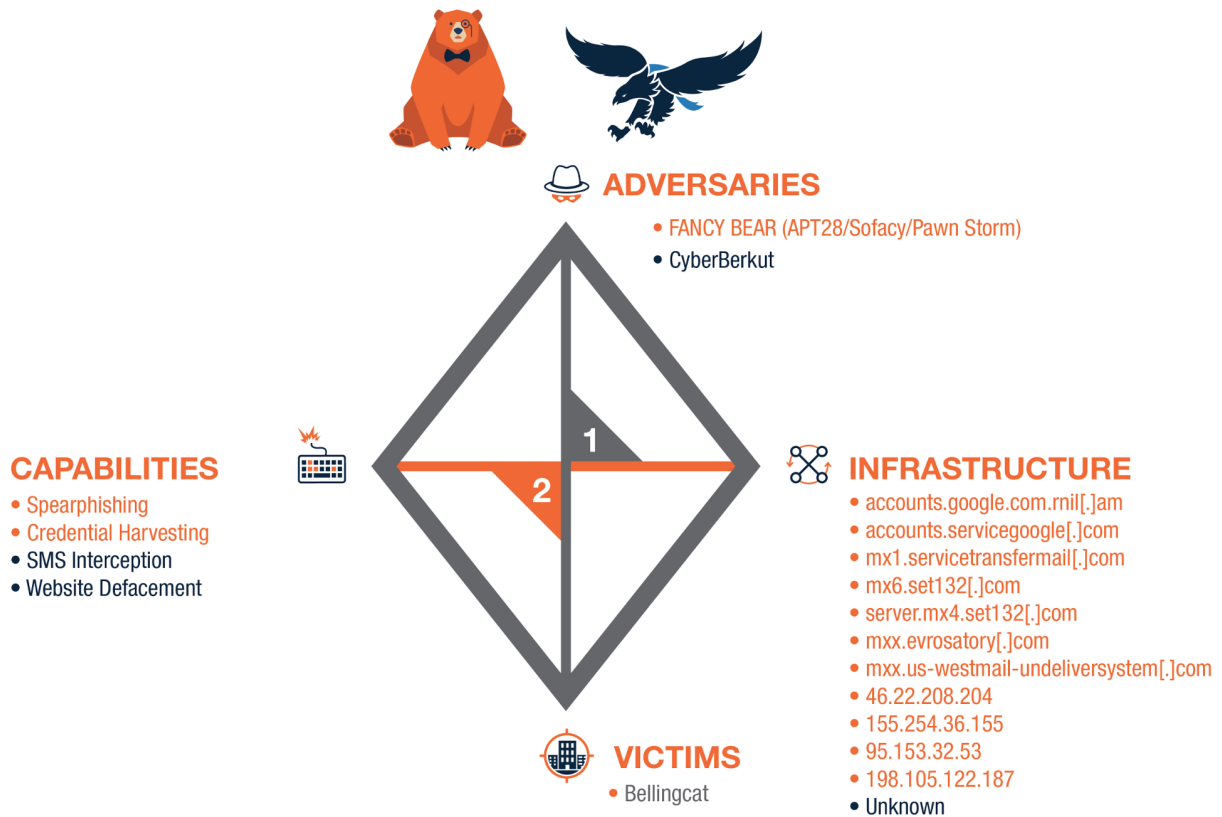
Read the full series of ThreatConnect posts following the DNC Breach: [“Rebooting Watergate: Tapping into the Democratic National Committee”](#), [“Shiny Object? Guccifer 2.0 and the DNC Breach”](#), [“What’s in a Name Server?”](#), [“Guccifer 2.0: the Man, the Myth, the Legend?”](#), [“Guccifer 2.0: All Roads Lead to Russia”](#), [“FANCY BEAR Has an \(IT\) Itch that They Can’t Scratch”](#), [“Does a BEAR Leak in the Woods?”](#), and [“Russian Cyber Operations on Steroids”](#).

### [UPDATE] October 7th 2016

#### Introduction

Since posting about the [DNC hack](#), each time we published a blog post on a BEAR-based topic we thought it was going to be our last. But like the Death Star’s gravitational pull, the story keeps drawing us back in as new information comes to light. Following our post on [DCLeaks as a Russian influence operation](#), [Bellingcat](#) founder [Eliot Higgins](#) reached out to us. Bellingcat, a group of citizen investigative journalists, has published articles critical of Russia and has been a key contributor to the international investigation of the shutdown of [Malaysian Airlines Flight 17 \(MH17\)](#) over Ukraine in 2014.

Higgins shared data with ThreatConnect that indicates Bellingcat has come under sustained targeting by Russian threat actors, which allowed us to identify a 2015 spearphishing campaign that is consistent with FANCY BEAR’s tactics, techniques, and procedures. We also analyzed a February 2016 attack by CyberBerkut — a group claiming to be pro-Russian Ukrainian hacktivists but also a suspected front for Moscow — against Russia-based Bellingcat contributor [Ruslan Leviev](#), where CyberBerkut defaced the Bellingcat website and leaked Leviev’s personal details. As evidenced by these efforts and [the attack on the World Anti-Doping Agency](#), organizations that negatively impact Russia’s image can expect Russian cyber operations intended to retaliate publicly or privately, influence, or otherwise maliciously affect them. The [Diamond Model](#) below summarizes the activity that Bellingcat experienced.



## Bellingcat Background

Bellingcat is a group of citizen investigative journalists — named after a classic fable — that uses open source information, such as photos and videos posted on social media, maps, and publicly available satellite imagery. Bellingcat articles have focused on a variety of current events in Africa, the Middle East, the U.S., and Europe with a specific focus on notable conflicts related to Syria, Ukraine, and Russia.

Bellingcat published its first post on July 5, 2014, and for the next twelve days focused mainly on the ongoing Syrian civil war, covering developments such as the use of chemical weapons, but also occasionally pointing out Russian involvement. On July 17, 2014, Malaysian Airlines Flight 17 crashed in pro-Russian rebel territory in eastern Ukraine and Bellingcat released their first post on the topic. Over the next two years, Bellingcat would publish no fewer than 92 posts from at least 8 contributors focused on Russian involvement in the downing of MH17, using open source information and imagery to prove the presence of the Russian military in eastern Ukraine and that a Russian-supplied Buk missile launcher shot down MH17 from pro-Russian rebel territory. The Kremlin vehemently denies this.

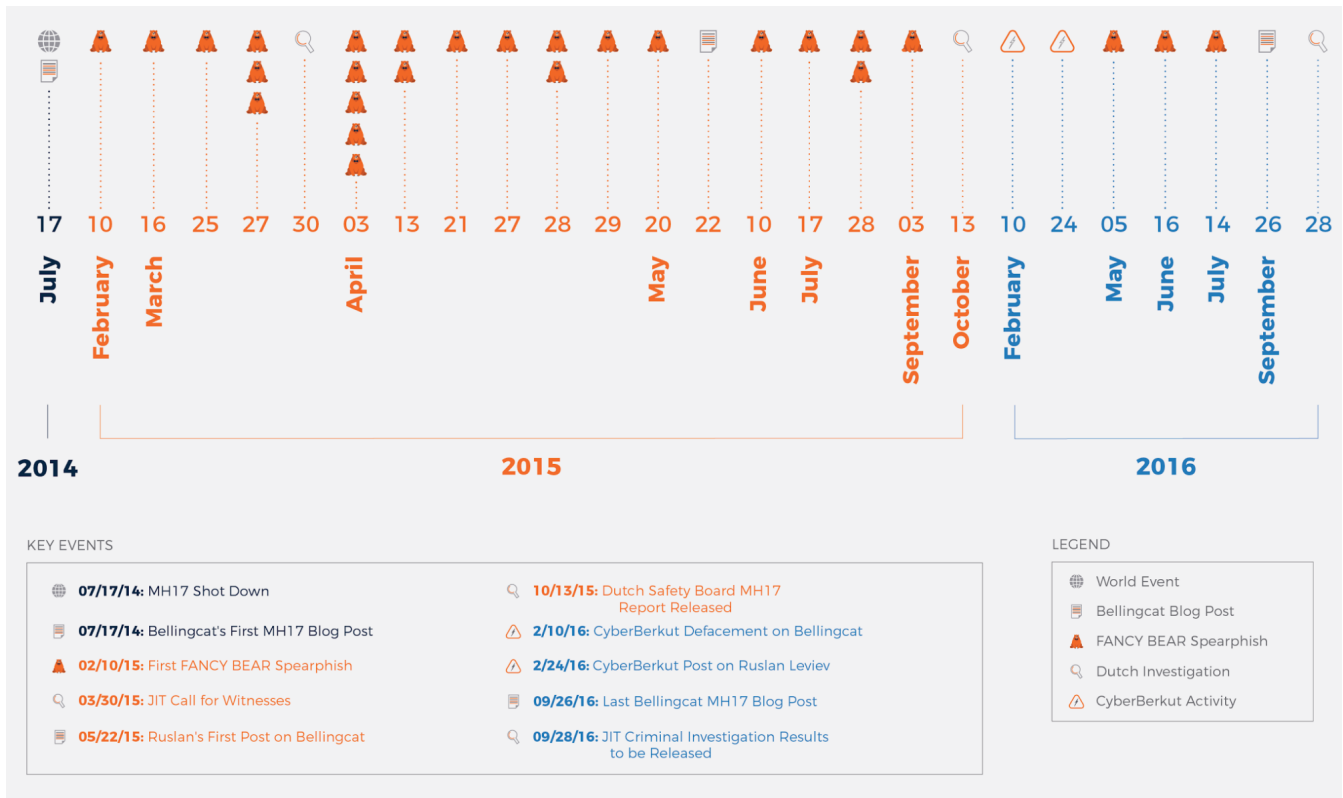
The Dutch took the lead in the criminal investigation through an international Joint Investigation Team (JIT) and officially considered Bellingcat's reporting in their investigation. Founder Eliot Higgins was included as an official witness. The Dutch Safety Board ultimately found MH17 was shot down by a Russian-made surface-to-air missile but declined to assign blame for who was responsible for the launch. On September 28, the JIT is due to release the results of their criminal investigation.

Compromising Bellingcat contributors could provide Russian intelligence services with journalists' contacts and sources, personal information, insight into future reporting perceived as indemnifying Russia, as well as sensitive personal information. Such collection could facilitate influence operations and retaliation efforts against Bellingcat, or access that could be leveraged for follow-on operations. Compromising Bellingcat contributors' accounts could also provide access to communications with the JIT, offering a glimpse at how the investigation of the downing of MH17 was proceeding.

## Activity Targeting Bellingcat

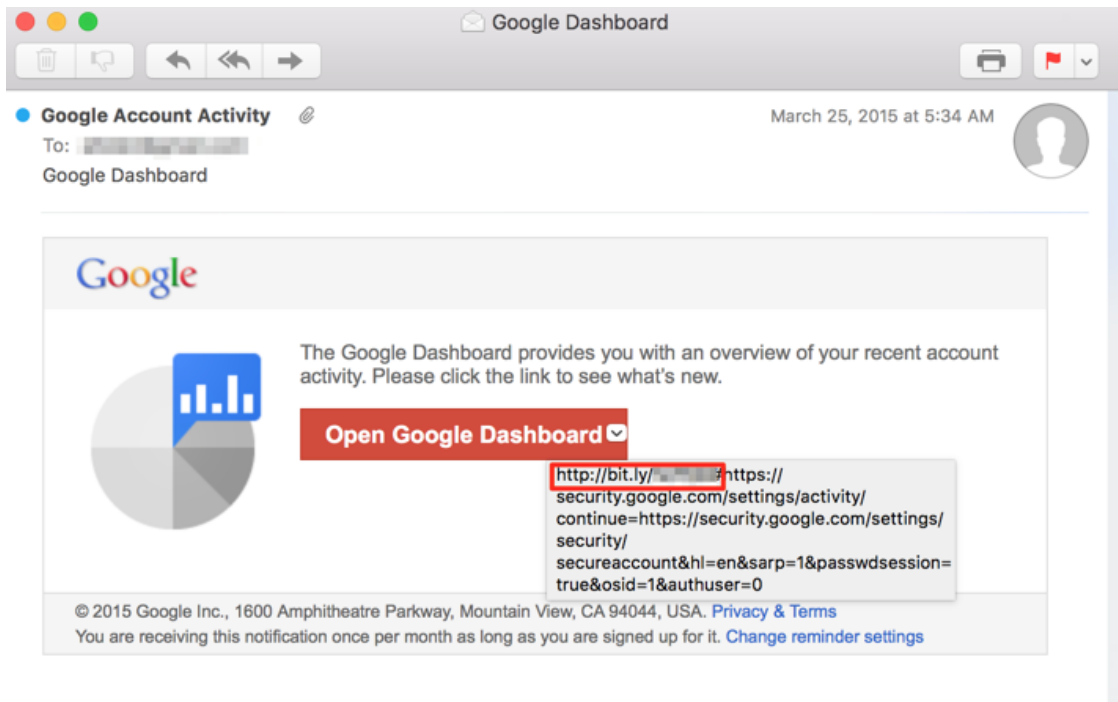
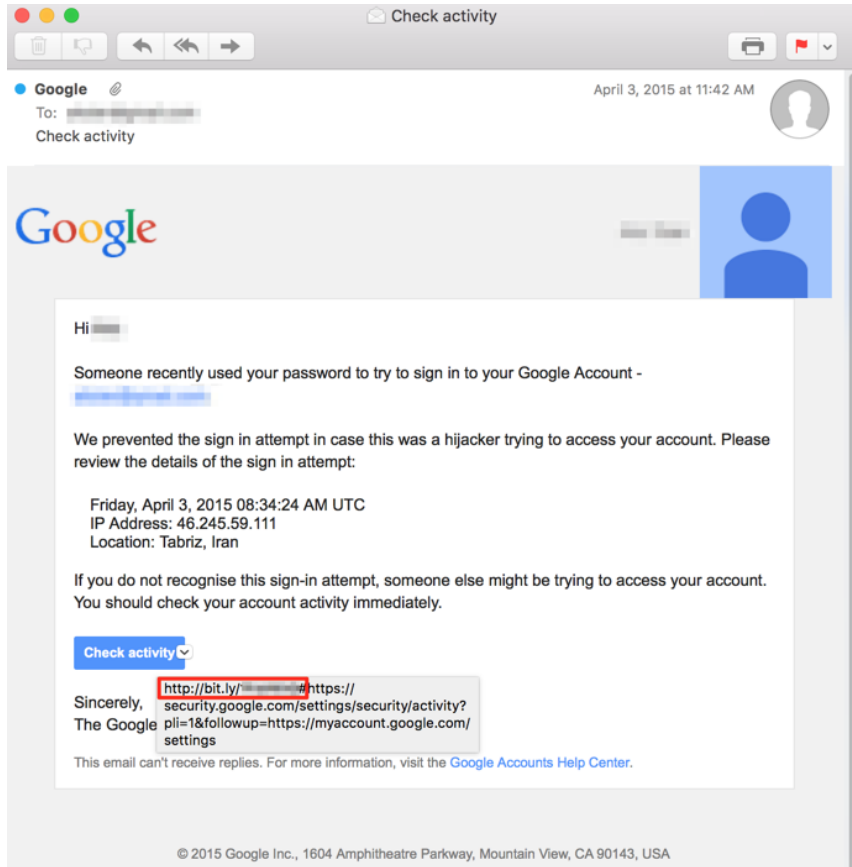
## Timeline

The timeline below summarizes the notable dates related to the MH17 crash and investigation, Bellingcat’s articles related to those events, and the malicious activity targeting Bellingcat and Leviev. It’s important to note we do not have complete insight into all of the malicious activity that may have targeted Bellingcat during this timeframe.



## FANCY BEAR



From February 2015 to July 2016 three researchers at Bellingcat — Higgins, Aric Toler, and Veli-Peka Kivimaki — who had contributed MH17 articles received numerous spearphishing emails, with Higgins alone receiving at least 16 phishing emails targeting his personal email account. A majority of the campaign took place from February to September 2015, with some activity resuming in May 2016. These spearphishing attempts consist of a variety of spoofed Gmail security notices alerting the target that suspicious activity was detected on their account. The target is prompted to click a URL resembling a legitimate Gmail security link to review the details of this suspicious activity. Below are screenshots of some of the spearphishing email targeting Bellingcat researchers.



New sign-in from Internet Explorer on Windows



Google, #@accounts.mailgoogle.com July 17, 2015 at 5:23 AM

To: [redacted]  
New sign-in from Internet Explorer on Windows



### New sign-in from Internet Explorer on Windows

Hi [redacted]  
Your Google Account [redacted] was just used to sign-in from Internet Explorer on Windows.

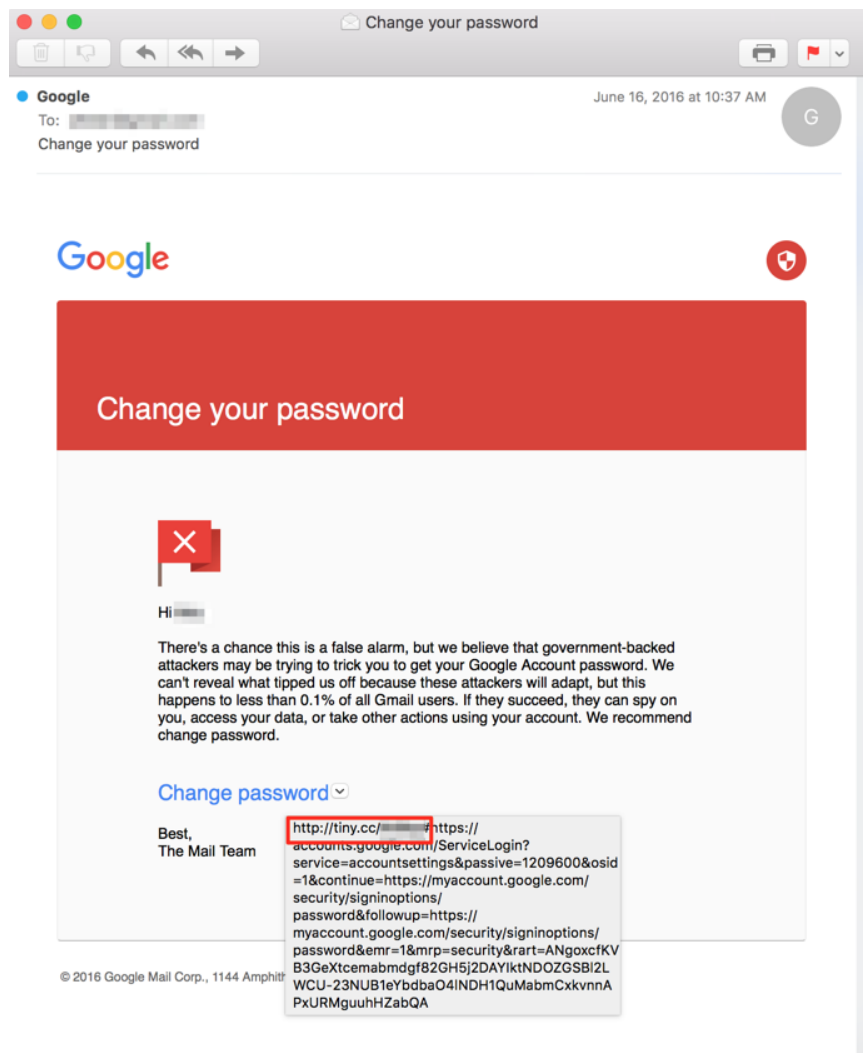


**Windows**  
Friday, 17 July, 9:20:30 UTC  
Internet Explorer

```
https://sites.google.com/site/[redacted]/  
sign-in-8#https://accounts.google.com/  
ServiceLogin?passive  
%1209600&osid=1&continue=https://  
myaccount.google.com/&followup=https://  
myaccount.google.com/  
&authuser=0&continue=https://  
security.google.com/settings/security/activity?  
pli=1
```

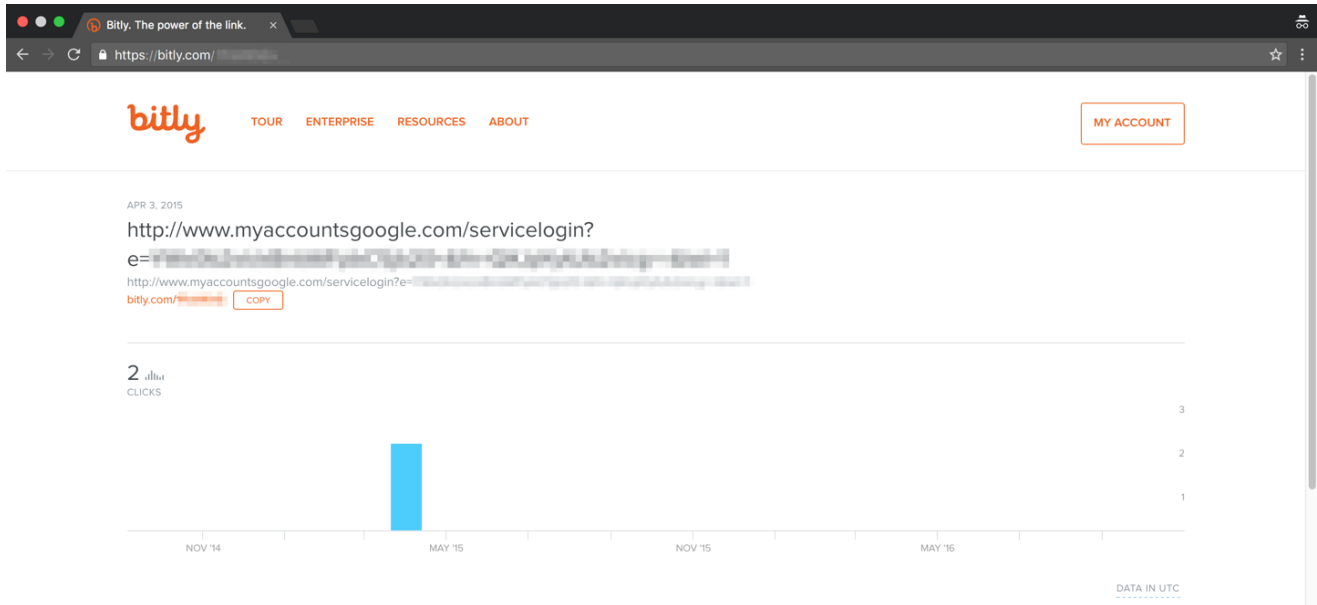
**Recognize this activity?**  
If you don't, please [review your devices and activity](#).

Why are we sending this? We take security very seriously and we want to keep you in the



The attackers used several methods to redirect the target to credential harvesting pages. In at least 21 of the emails, the URL redirects the victim to a shortened Bitly URL. These shortened Bitly links, in turn, direct the victim to another Google-spoofing URL appended with the [base64](#) encoded target email and name. One of the emails used a shortened TINYCC URL to achieve the same effect. In four of the other emails, the security links direct the target to a Google Sites page that spoofs a Google login page. Once the target visits the Bitly, TINYCC, or Google Sites URLs, they are prompted to enter their Google credentials, which would then be captured by the threat actors.

The specifically crafted URLs with target-specific strings are consistent with a FANCY BEAR technique highlighted in [Dell Secureworks research](#) and [employed against a DNC staffer](#) whose files were leaked on DCLeaks. Reviewing the click information for the Bitly links, we identified that at least three of the Bitly URLs targeting the same Bellingcat individual were accessed in the timeframe consistent with the spearphishing attack. This suggests the individual clicked on the links in three of the spearphishing messages, but Bellingcat confirms that no credentials were supplied to these pages.



Other consistencies with Russia and FANCY BEAR activity were also identified. In early May and again in mid-June 2016 the Bellingcat contributor Aric Toler’s personal email address was targeted by FANCY BEAR. Using ThreatConnect’s Email Import function, we are able to identify that both messages abused Moscow-based Yandex email services to send malicious emails to the researcher. In the May phishing example FANCY BEAR used the Yandex account berg01berg01@yandex[.]com.

THREATCONNECT DASHBOARD BROWSE ANALYZE SPACES CREATE IMPORT Search

Import E-mail

Import Score Indicators Victims Confirm

**Indicators**

Header ▾

- Doesn't Exist in ThreatConnect
- Exists in ThreatConnect
- Shared in ThreatConnect

Return-Path: <berg01berg01@yandex.com>

Received: from forward12h.cmail.yandex.net (forward12h.cmail.yandex.net. [87.250.230.154])

Thu, 05 May 2016 00:48:19 -0700 (PDT)

Received-SPF: pass (google.com: domain of berg01berg01@yandex.com designates 87.250.230.154 as permitted sender) client-ip=87.250.230.154;

Received: from smtp4h.mail.yandex.net (smtp4h.mail.yandex.net [84.201.186.21])

for <...>; Thu, 5 May 2016 10:48:19 +0300 (MSK)

Received: from smtp4h.mail.yandex.net (localhost [127.0.0.1])

for <...>; Thu, 5 May 2016 10:48:17 +0300 (MSK)

**Indicator List**

**Existing**

**New**

berg01berg01@yandex.com

**Excluded**

- 10.182.111.65 (Address-IPv4 in header, system-wide rule)
- mail-lf0-x22a.google.com (Host in header, system-wide rule)
- mail-lf0-x22a.google.com (Host in header, system-wide rule)
- mail-lf0-x22a.google.com (Host in header, system-wide rule)
- 10.112.167.103 (Address-IPv4 in header, system-wide rule)
- 127.0.0.1 (Address-IPv4 in header, system-wide rule)

< Back > Next SAVE

In the June 2016 example, Toler was targeted with a message that used hellomail1@yandex[.]com in a manner consistent with how Billy Rinehart was targeted prior to content from his personal Gmail being posted to DCLeaks.

The screenshot displays the ThreatConnect 'Import E-mail' workflow. The 'Indicators' step is highlighted, showing a list of email headers on the left and an 'Indicator List' on the right. The 'Indicator List' includes 'Existing' (none), 'New' (hellomail1@yandex.com), and 'Excluded' (various IP addresses and URLs).

By analyzing the email headers provided by Bellingcat, we identified domains and corresponding IP addresses that the attackers leveraged as part of the spearphishing operation. The table below also shows the registrant for the domain, the creation date for the WHOIS record, and the name server the domain used during the attack timeframe.

Spearphishing Domain	Mailserver IP	Domain Registrant	Domain Create Date	Name Server During Attack
mxx.evrosatory[.]com	46.22.208.204	andre_roy@mail.com	2/13/14	Carbon2u.com
accounts.servicegoogle[.]com	155.254.36.155	theforeignnews@gmail.com	5/22/15	Cata501836.earth.orderbox-dns.com
mxx.us-westmail-undeliversystem[.]com	46.22.208.204	andre_roy@mail.com	2/28/14	Carbon2u.com
mx1.servicetransfermail[.]com	95.153.32.53	theforeignnews@gmail.com	6/3/15	Cata501836.earth.orderbox-dns.com
accounts.google.com.rnil[.]am	198.105.122.187	Private	7/7/14	Carbon2u.com
mx6.set132[.]com	198.105.122.187	emmer.brown@mail.com	9/30/14	Carbon2u.com
server.mx4.set132[.]com	46.22.208.204	emmer.brown@mail.com	9/30/14	Carbon2u.com

The domains evrosatory[.]com,us-westmail-undeliversystem[.]com have been previously identified by Pricewaterhouse Coopers as FANCY BEAR, and the domain servicetransfermail[.]com closely resembles the servicetransfermail[.]com infrastructure that German Intelligence (BvF) established as FANCY BEAR within Cyber Brief Nr. 01/2016.

FANCY BEAR also previously used both the Cata501836 and Carbon2u name servers to host infrastructure and email addresses from 1&1's mail.com to register domains. We were able to identify further overlaps with other FANCY BEAR infrastructure by pivoting off of these indicators, which we will describe in a later blog post. Based on these



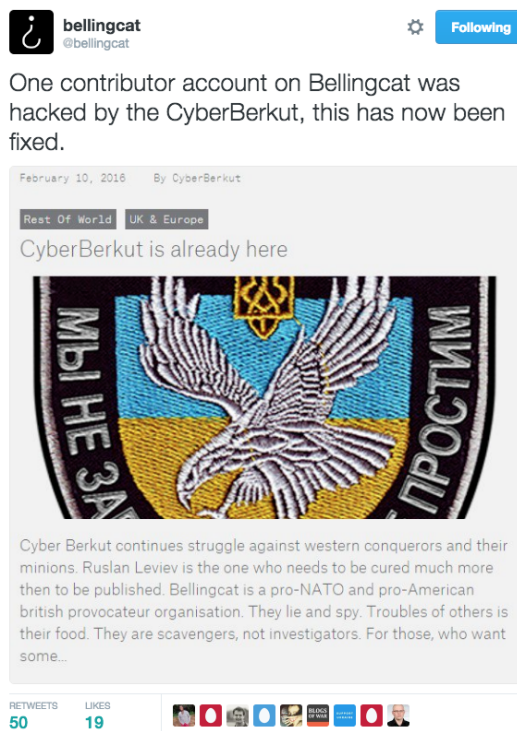
consistencies, we assess FANCY BEAR almost certainly is behind the spearphishing and credential harvesting campaign targeting Eliot Higgins and other Bellingcat researchers.

### CyberBerkut Activity

CyberBerkut describes itself as a group of pro-Russian Ukrainian hackers. They borrow the “Berkut” name from the now disbanded Ukrainian riot police who responded brutally to the 2014 EuroMaidan demonstrations in Kiev. CyberBerkut runs a digitally-fueled, aggressive, active measures campaign directed against a pro-western government in Kiev and points of western influence — such as NATO — in eastern Europe.

CyberBerkut has conducted attacks across a spectrum of technical sophistication including distributed denial of service attacks (DDOS), disrupting and degrading the networks of Ukraine’s Central Election Commission during the 2014 election, hacking Ukrainian billboards and displaying pro-Russian messages, conducting computer network exploitation and strategic leaks of emails and documents, and leaking intercepted phone calls between high ranking Ukrainian officials. This range suggests highly capable actors are behind CyberBerkut and they employ a high degree of operational planning when considering the offensive use of information and their effects.

CyberBerkut defaced the Bellingcat webpage on February 10, 2016, claiming credit for the attack and singling out Ruslan Leviev, a Russian opposition blogger and Bellingcat contributor.



Leviev published a compelling piece of citizen journalism on May 22, 2015 exploring the fate of Russian Spetsnaz soldiers believed to have been killed in combat operations within Ukraine earlier that month. According to Bellingcat founder Higgins, Leviev’s contributor account was compromised and used to post the CyberBerkut message. In an email interview, Leviev makes the following statement regarding the events that led to the compromise of his credentials and the defacement.

*In my case, my old email account, which was located on Yandex servers, was hacked. The email account had a long, difficult password, not a word, from various letters, numbers, and special symbols. Plus there was a telephone number bound to the account for second factor authentication.*

*Exactly how it was hacked — I don’t know.*

1. *Either they as employees, or with their active assistance, intercepted the SMS authentication code.*

2. Or they, again, as an officer from the authorities or with their active assistance, gained direct access to the Yandex Mail servers where they seized the email from my old inbox.
3. Or they know about a vulnerability in Yandex email that nearly nobody else knows about.

*Having seized the old email inbox, they used the password recovery mechanism for LiveJournal. My LiveJournal account (which I have not used for a long time) was connected to my old email address, but LiveJournal does not provide second factor authentication. Via password recovery of my LiveJournal from my stolen email, they took over my LiveJournal account and made a post.*

*In the same stolen email account, they found my username and password for my account at Bellingcat (I had once published an investigation directly on the Bellingcat website) and they published a post there in my name.*

*At the same time, my icloud account was not setup for second factor authentication, and was connected only to my old email address for password recovery, it was also taken over. They performed a password recovery via my stolen email address for icloud, logged in, but I received a notification on my iPhone about it, and I quickly cut off their access, but they were able to download some photos.*

*They also tried to hack my Facebook and Twitter. They were unable to crack Facebook, because I had second factor authentication and always need to enter the code generated by the Facebook app. They were able to login to Twitter and change the password but nothing was deleted and they didn't tweet anything. I restored the password.*

*Based on all the data, I assume that, as in the case of Albuovym, Kozlovsky, Parkhomenko, this was the activity of security services who intercepted the SMS containing the access code. So they got access to my old email account and they also gained access to my Twitter account (which was also under two-factor, but code is sent via SMS rather than generated in an app).*

*Of my social networks where two-factor codes are generated via an application, they were unable to crack. Of my social networks where the two-factor code was sent via SMS, they were able to crack.*

Leviev suggests the attackers had direct access to Yandex mail servers or were able to intercept the SMS message used for two factor authentication to compromise his old Yandex email account. Leviev goes on to describe that the actors then used emails from that old account to compromise his iCloud account and access pictures and other information saved from Leviev's phone to iCloud. Some of this information was ultimately put in a February 24, 2016 post on CyberBerkut's website that contained sensitive details of Leviev's personal life, such as his pictures, phone number, address, passport scan, girlfriend's name, and dating and sexual preferences.

These attacks were an overt attempt to discredit Bellingcat research and Leviev, but also carried a message to others who publicly voice positions critical of Moscow that this form of journalism does not go unnoticed. We also found it interesting how much effort was expended and the degree of sources and methods exposed to achieve a simple defacement. We do not know whether the attackers intercepted Leviev's SMS-based two-factor authentication or had direct access to Yandex mail servers, but either tactic is more suggestive of a state-backed actor as opposed to independent hacktivists.

## **CyberBerkut and FANCY BEAR: Not the Same, But Showing Up to the Same Party**

---

Throughout our research, we have focused on FANCY BEAR, an advanced persistent threat (APT) group assessed to be Russian government. CyberBerkut, on the other hand, was a referential data point when we looked at precedence for pro-Russian proxies interfering with elections. CrowdStrike assessed in its [2015 Global Threat Report](#) "there are indications that CyberBerkut has ties to Russian state security," but the degree of Russian government control over the group is disputed.

The timing of the FANCY BEAR spearphishing campaigns and the CyberBerkut attack against Leviev are interesting. The concerted FANCY BEAR spearphishing efforts over a six month timeframe in 2015 shows Moscow's clear intent to compromise Bellingcat, most likely due to their posts on key current events involving Russia. This activity was followed by a hard stop and then additional targeted efforts by CyberBerkut in early 2016, which was in-turn followed by additional FANCY BEAR spearphishing from May to July 2016. A key assumption underlying any assessment about how these activities are related stems from how an analyst assesses the motives for targeting Leviev.

We came up with two scenarios:

*Stronger/Closer Coordination Between FANCY BEAR and CyberBerkut.* In this scenario, the activities against Bellingcat are coordinated with these two entities handing off operations. The timing suggests that the state actors, looking to compromise Bellingcat, pivoted to a more aggressive attack against Leviev when the initial spearphishing campaign failed to yield the desired results. Leviev is targeted more aggressively as a means to get at Bellingcat and since he lives in Russia, state actors would have additional tools in their kit to intercept his SMS two-factor authentication messages or gain direct access to Yandex's mail servers. In this scenario, CyberBerkut functions as much as a strategic messaging outlet as the actual attacker and is subject to a much greater degree of direction and control from Moscow than previously assessed.

*The Common Enemies Approach: Weaker/Less Coordination Between FANCY BEAR and CyberBerkut.* In this scenario, the spearphishing campaigns conducted by FANCY BEAR are distinct in purpose and perpetrator from the CyberBerkut attack against Leviev. The spearphishing campaigns are more focused on Bellingcat's coverage of the MH17 shootdown and involvement in the JIT investigation. CyberBerkut targets Leviev separately after his coverage of Russian military involvement in eastern Ukraine with some assistance from supportive friends in Moscow to compromise his Yandex account. Targeting Leviev is less about a broader compromise of Bellingcat and more about harassing one journalist. In this scenario, CyberBerkut is advancing Moscow's interests and can call on the Russian intelligence services, but is still a distinct group.

## Leak Sites Leaking Over

---

We looked to see if we could identify other overlaps between FANCY BEAR and CyberBerkut that would help us assess which of these two scenarios was more likely. Through our research into the Bellingcat activity, we found some surprising content overlaps with DCLeaks — another assessed Russian influence outlet — and a CyberBerkut pattern of registering infrastructure that FANCY BEAR also uses. These developments move the needle slightly towards a more coordinated relationship between the two groups, but not decisively.

### *Comparing DCLeaks and CyberBerkut*

In [our previous post](#), we identified a website called DCLeaks as a Russian-backed influence outlet. Information shared with ThreatConnect indicates that there is an association of some kind between the Guccifer 2.0 persona and the DCLeaks website. Shortly after publication, we became aware of a cache of documents leaked on the DCLeaks site. The files were allegedly obtained via a compromise of an organization affiliated with George Soros. It is interesting to note that earlier in 2016 CyberBerkut also published files purportedly associated with Soros.

Analysis conducted by [Anton Cherepanov](#), a security researcher who works for ESET, suggests that the content of the two leaks are similar with at least [three of the Soros documents](#) being found on both sites. The acquisition and publication of documents belonging to, or in some way associated with, the same individual is of interest as overlaps in targeting and potential similarities in stolen content could be indicative of a connection between DCLeaks and CyberBerkut. Further, as we have identified that there is a connection from DCLeaks to Guccifer 2.0 and from Guccifer 2.0 to FANCY BEAR, the overlap in leaked documents may suggest that both leak sites obtained their data from the same collection source, FANCY BEAR.

While this alone isn't enough to verify a relationship between the sites, there are some other interesting similarities. Despite their statuses as a U.S.-focused whistleblower and hacktivist group respectively, the websites of both DCLeaks and CyberBerkut primarily host content that is critical of individuals and governments perceived to oppose Russian foreign and domestic policies. Both sites attempt to appeal to civilian masses in the U.S. and Ukraine respectively by calling attention to purported in the political systems.

### *Aleksandr Panchenko*

CyberBerkut's main domain, cyber-berkut[.]org, was registered using privacy protection through the registrar Internet.bs and shortly thereafter hosted using CloudFlare infrastructure. Several other CyberBerkut-related domains redirect to this website. Most of these domains were also registered using privacy protection, but one domain, cyber-berkut[.]net was

registered by “Aleksandr Panchenko” using the email address alex\_panchenko@mail[.]com. The same day the domain was registered through Reg.ru, it was later routed to CloudFlare infrastructure, suggesting that this domain was not opportunistically procured by a domain registrant in hopes they could sell it to the CyberBerkut actors.

```
Domain name: cyber-berkut.net
Domain idn name: cyber-berkut.net
Registry Domain ID:
Registrar WHOIS Server: whois.reg.ru
Registrar URL: https://www.reg.com/
Registrar URL: https://www.reg.ru/
Registrar URL: https://www.reg.ua/
Updated Date: 2014-07-04
Creation Date: 2014-07-04T09:23:16Z
Registrar Registration Expiration Date: 2015-07-04
Registrar: Domain names registrar REG.RU LLC
Registrar IANA ID: 1606
Registrar Abuse Contact Email: abuse@reg.ru
Registrar Abuse Contact Phone: +7.4955801111
Registry Registrant ID:
Registrant Name: Aleksandr Panchenko
Registrant Organization: Private Person
Registrant Street: Uzbeksкая
Registrant City: Chernovtsi
Registrant State/Province: Chernovtsi
Registrant Postal Code: 58021
Registrant Country: UA
Registrant Phone: +380991405443
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: alex_panchenko@mail.com
```

Additional research into this name and email address identifies six other CyberBerkut-related domains, none of which are active currently, registered by this individual:

- Cyber-berkut[.]su
- Cyber-berkut[.]tk
- Cyber-berkut[.]us
- Cyber-berkut[.]me
- Cyber-berkut[.]cz
- Cyber-berkut[.]im

While certainly not definitive, the use of a mail.com email address to register domains is consistent with recently identified FANCY BEAR registration activity against the [DCCC](#), [WADA](#), and [CAS](#).

## Tracing out FB Infrastructure Based on Bellingcat Input

---

The activity that Bellingcat alerted us to provided a plethora of domains, IP addresses, email addresses, and other registration and hosting information for us to pivot off of to identify other pertinent infrastructure. In an upcoming blog post, we'll seek to identify as much FANCY BEAR infrastructure and aliases as possible using the ThreatConnect platform and capabilities from some of our industry partners.

Reviewing the CATA501836 and Carbon2u name servers, we were able to identify dozens of active domains that fit the FANCY BEAR mold and likely spoof organizations that Moscow would seek to compromise.

Pivoting off of Bellingcat's email headers we were able to identify hundreds of domains and IPs, and dozens of email addresses and aliases most likely used by FANCY BEAR, some of which were not previously identified. This review primarily identified historical FANCY BEAR information, but the conclusions from it help verify FANCY BEAR TTP assessments, provide additional targeting context, and may be useful in retrospective reviews of malicious activity.

## Conclusion

The campaign against Bellingcat provides yet another example of sustained targeting against an organization that shines a light on Russian perfidy. The spearphishing campaign is classic FANCY BEAR activity while CyberBerkut's role raises yet more questions about the group's ties to Moscow. These end-to-end cyber operations begin with targeting and exploitation and end with strategic leaks and other active measures employed against those with whom they disagree.

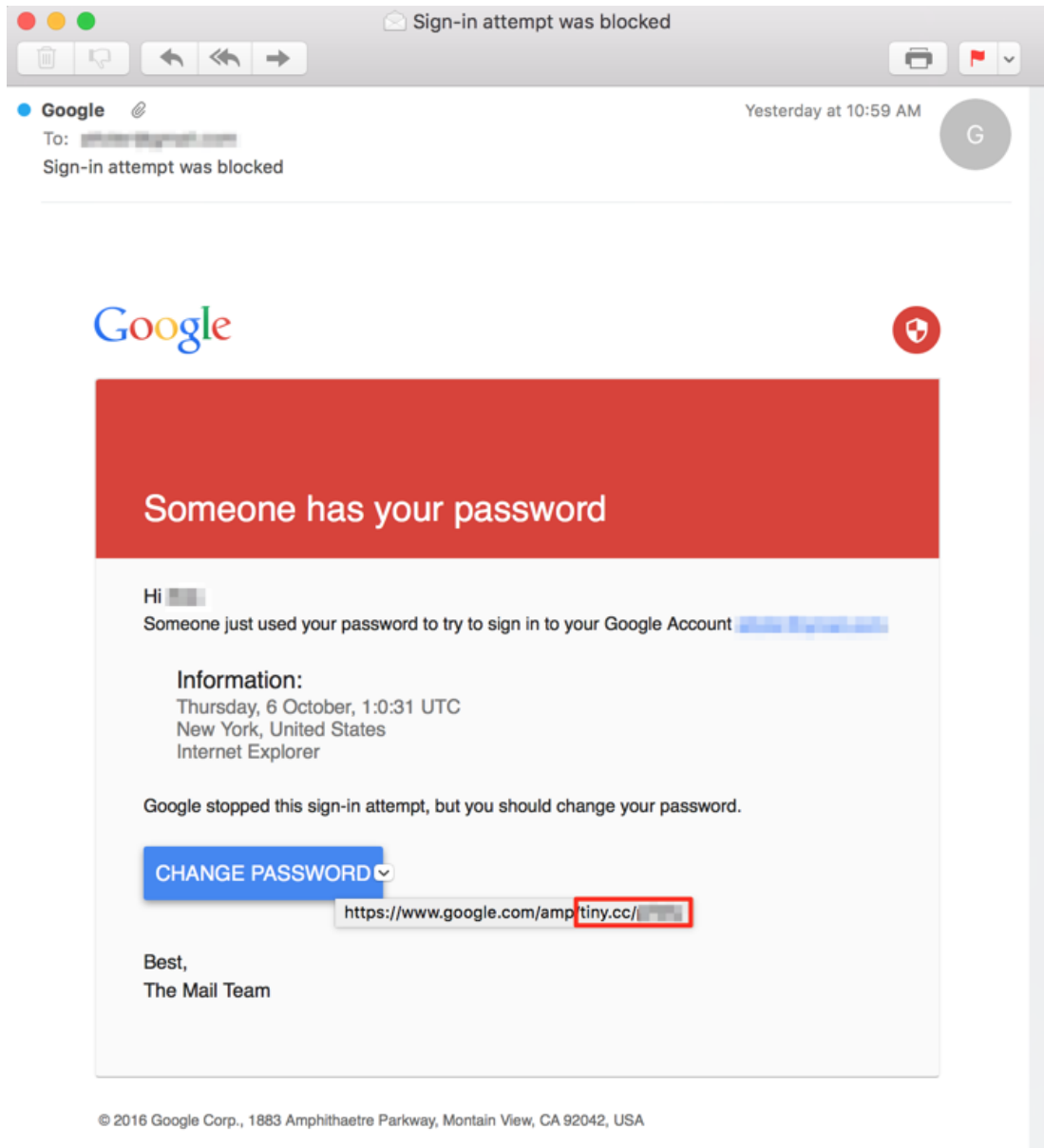
These efforts go above and beyond traditional intelligence requirements such as gaining insight into a sensitive project or sources. Vilifying the messenger and dumping their personal data is part of the game, intended to intimidate and embarrass those that speak ill of Moscow. If Russia is willing to go to these lengths to compromise a small journalist organization and its contributors, consider what they are willing to do to major news and media outlets that publish similar articles. While many organizations remain reticent to share information, this knowledge is the prerequisite to establishing how widespread such efforts are and the adversary's *modus operandi*.

The BEARs win if their active measures campaigns push, scare, or intimidate their targets into doing what they want. If you encounter a BEAR, you're doing something right. Don't back down. And turn on two-factor authentication for everything.

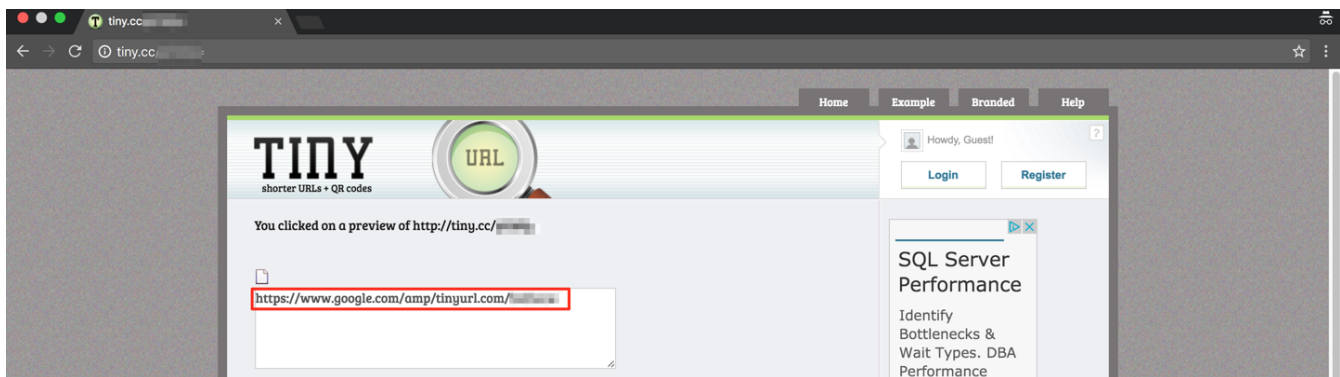
## Update

---

On October 5 2016, probable FANCY BEAR actors again sent a spearphishing message to a Bellingcat contributor. This spearphishing message spoofed Google security services, similar to those previously used to target Bellingcat.



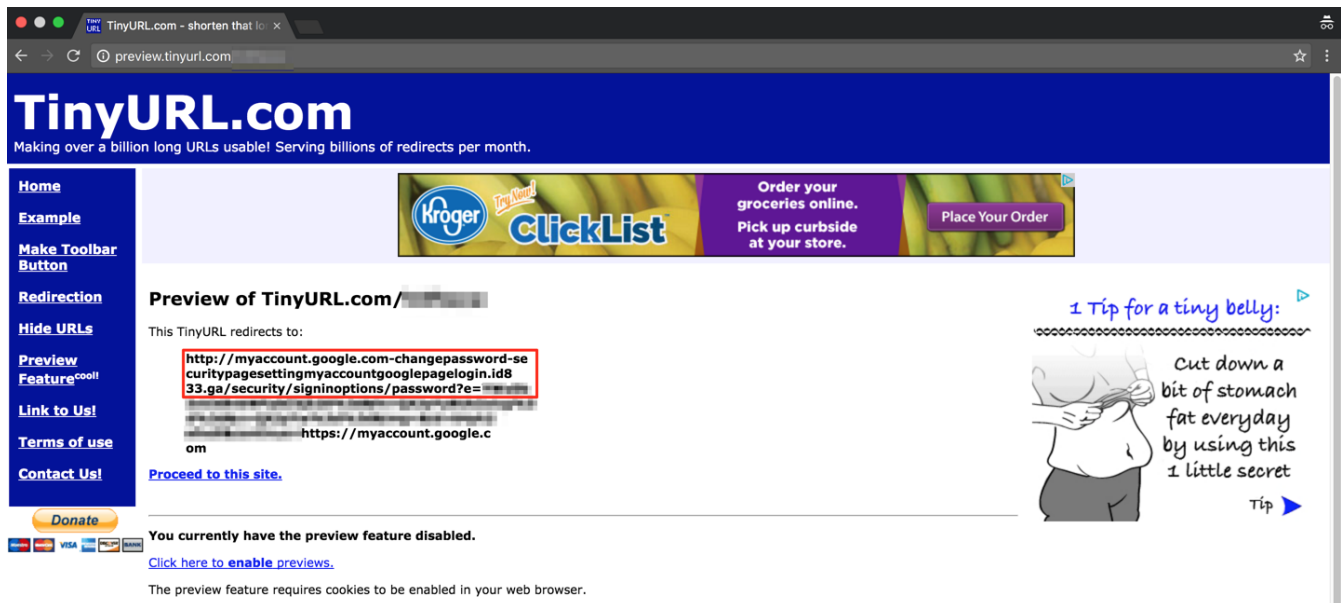
FANCY BEAR used a shortening service to mask the malicious link, similar to the previous messages, but it appears the actors attempted to obfuscate their activity by using two separate shortening services to hide the final malicious link. The tiny.cc link that is in the spearphishing message actually points to a TinyURL shortened URL.



The TinyURL in turn points to the below URL:

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

This URL is appended with a target-specific base64 encoded string as was seen in the previous spearphishing messages targeting Bellingcat and others.



The id833[.]jga domain is hosted at the 89.40.181[.]119 IP (Bucharest, RO) which also hosts the domain id834[.]jga. There is a subdomain for the id834[.]jga similar to the URL above that is also hosted at the same IP. This suggests that the id834[.]jga domain has also been operationalized, though we have no information indicating who has been targeted with it. The WHOIS records for these domains did not contain any additional information on the registrants or other domains they may have registered.

Using ThreatConnect's Email Import feature, we identified that the spearphishing message was sent through Yandex mail servers using the email address g.mail2017@yandex[.]com.

ThreatConnect Import E-mail

https://app.threatconnect.com/auth/email/modification/index.xhtml

DASHBOARD BROWSE ANALYZE SPACES CREATE IMPORT Search

Import E-mail

Import Score Indicators Victims Confirm

**Indicators**

Header

Doesn't Exist in ThreatConnect  
Exists in ThreatConnect  
Shared in ThreatConnect

Return-Path: <hellomail1@yandex.com>

Received: from forward12j.cmail.yandex.net (forward12j.cmail.yandex.net [5.255.227.176])  
Thu, 16 Jun 2016 07:37:15 -0700 (PDT)

Received-SPF: pass (google.com: domain of hellomail1@yandex.com designates 5.255.227.176 as permitted sender) client-ip=5.255.227.176

Received: from smtp13.mail.yandex.net (smtp13.mail.yandex.net [95.108.130.68])  
for < >; Thu, 16 Jun 2016 17:37:08 +0300 (MSK)

Received: from smtp13.mail.yandex.net (localhost [127.0.0.1])  
for < >; Thu, 16 Jun 2016 17:37:08 +0300 (MSK)

Received: by smtp13.mail.yandex.net (nsmtp/Yandex) with ESMTPSA id BRqFjQWhu-

**Indicator List**

**Existing**

**New**  
hellomail1@yandex.com

**Excluded**

10.107.143.147 (Address-IPv4 in header, system-wide rule)  
mail-wm0-x22e.google.com (Host in header, system-wide rule)  
mail-wm0-x22e.google.com (Host in header, system-wide rule)  
mail-wm0-x22e.google.com (Host in header, system-wide rule)  
10.28.222.136 (Address-IPv4 in header, system-wide rule)  
127.0.0.1 (Address-IPv4 in header, system-wide rule)  
https://lh3.googleusercontent.com/ (Url in body, organization-specific rule)  
https://lh3.googleusercontent.com/ (Url in body, organization-specific rule)  
http://tiny.cc https://accounts.google.com/ServiceLogin?service=accountsettings&passive=1209600&osid=1&continue=https://myaccount.google.com/security/signinoptions/password&followup=https://myaccount.google.com/security/signinoptions/password&emr=1&mrp=security&rart=ANgoxcfkVB3GeXtcemabmdgf82GH5j2DAYlktNDOZGSBI2LWCU (Url in body, system-wide rule)

< Back > Next

This was the first identified spearphish against Bellingcat since July 2016 and suggests that FANCY BEAR activity against them is ongoing. Other organizations involved in the MH17 investigation that would draw Moscow's ire should be on the lookout for similar activity.