August 19, 2016

Russian Cyber Operations on Steroids

In Blog, Featured Article, Threat Research

Russian Cyber Operations On Steroids

ThreatConnect Identifies FANCY BEAR Ties to World Anti-Doping Agency Phishing

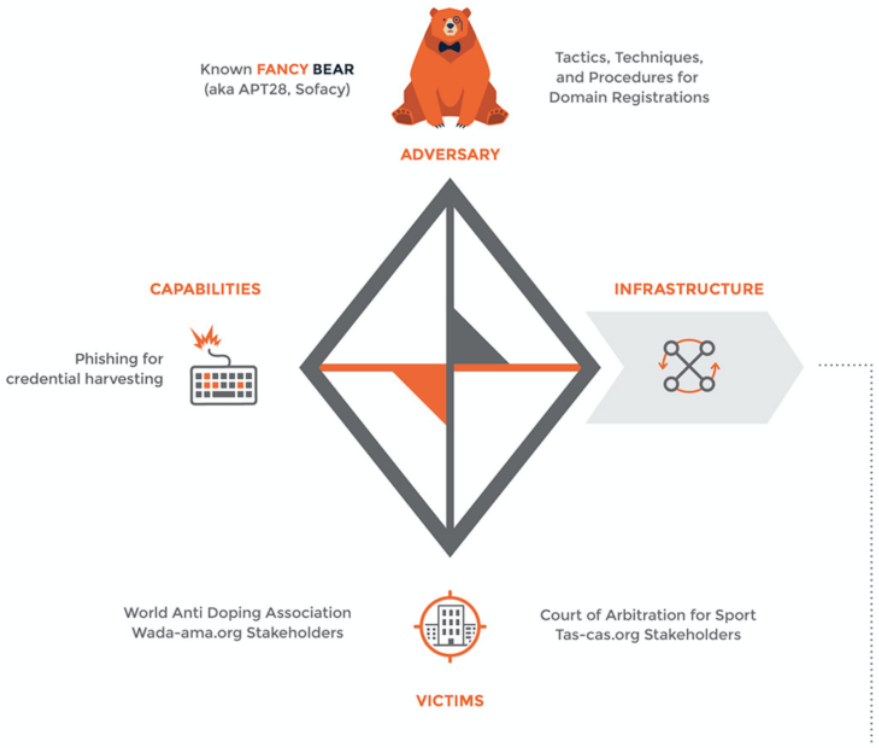
Read the full series of ThreatConnect posts following the DNC Breach: "Rebooting Watergate: Tapping into the Democratic National Committee [https://www.threatconnect.com/tapping-into-democratic-national-committee/]", "Shiny Object? Guccifer 2.0 and the DNC Breach [https://www.threatconnect.com/guccifer-2-0-dnc-breach/]", "What's in a Name Server? [https://www.threatconnect.com/whats-in-a-name-server/]", "Guccifer 2.0: the Man, the Myth, the Legend? [https://www.threatconnect.com/reassesing-guccifer-2-0-recent-claims/]", "Guccifer 2.0: All Roads Lead to Russia [https://www.threatconnect.com/guccifer-2-all-roads-lead-russia/]",

"FANCY BEAR Has an (IT) Itch that They Can't Scratch [https://www.threatconnect.com/fancy-bear-it-itch-they-cant-scratch/] ", "Does a BEAR Leak in the Woods? [https://www.threatconnect.com/blog/does-a-bear-leak-in-the-woods/] ", "Russian Cyber Operations on Steroids [https://www.threatconnect.com/blog/fancy-bear-anti-doping-agency-phishing/] ", and "Can a BEAR Fit Down a Rabbit Hole? [https://www.threatconnect.com/blog/state-board-election-rabbit-hole/] ".

On August 15, the World Anti-Doping Agency (WADA) alerted stakeholders [https://m.paralympic.org/news/wada-warns-stakeholders-phishing-scams] to phishing emails that used domains spoofing the WADA's legitimate domain, wada-ama.org. WADA confirmed [https://www.wada-ama.org/en/media/news/2016-08/wada-confirms-illegal-activity-on-yuliya-stepanovas-adams-account] that some users had received illegitimate credential harvesting e-mails that look as though they came from the WADA. The domains in the alert included:

- **wada-awa[.]org**
- **wada-arna[.]org**

ThreatConnect's Research team reviewed these domains and found that the sites were recently registered and their registration and hosting information are consistent with Russian FANCY BEAR tactics, techniques, and procedures (TTPs), as shown in the diamond model below. Further, we also identified another domain registered by the same individuals -- **tas-cass[.]org** -- that spoofs the Court of Arbitration for Sport's (CAS) legitimate tas-cas.org domain.



WADA's alert follows news from mid-August that WADA accounts and servers had been compromised. On August 11, a group identifying themselves as Anonymous Poland (@anpoland) defaced the CAS website [http://www.dailydot.com/layer8/world-anti-doping-agency-hackers/] and leaked data stolen from WADA and CAS servers [https://www.hackread.com/world-anti-doping-agency-site-hacked/] . On August 13, the WADA [https://www.wada-ama.org/en/media/news/2016-08/wada-confirms-illegal-activity-on-yuliya-stepanovas-adams-account] and email [https://www.theguardian.com/sport/2016/aug/13/russian-whistleblower-yuliya-stepanova-hacked-wada] accounts belonging to Yuliya Stepanova, the Russian athlete who was called "Judas [http://www.nytimes.com/2016/07/02/sports/olympics/yuliya-stepanova-rio-olympics.html] " by Vladimir Putin for helping to blow the whistle on the state sponsored doping scandal, were hacked.

We assess that the phishing and Stepanova's compromise most likely are part of targeted activity by Russian actors in response to the

whistleblower and the WADA's recommendation to ban all Russian athletes from the Olympic and Paralympic games in Rio de Janeiro, Brazil. Successful operations against these individuals and organizations could facilitate Russian efforts to privately or publically intimidate them or other potential whistleblowers. At this time, we are skeptical of @anpoland's origins but cannot determine the extent to which, if any, they are a Russian platform similar to Guccifer 2.0 or DCLeaks.

ThreatConnect made a concerted effort to alert WADA and CAS to these findings and have shared indicators from this activity in ThreatConnect's Incident 20160818A: Activity Targeting the WADA and CAS [https://app.threatconnect.com/auth/incident/incident.xhtml?incident=1412887] .

WADA and CAS Background

An international independent agency, the WADA [https://www.wada-ama.org/en] is not only composed of, but funded by governments and the sport movement worldwide. One of the organization's primary responsibilities is to monitor the World Anti-Doping Code [https://www.wada-ama.org/en/what-we-do/the-code] .

The CAS [http://www.tas-cas.org/en/index.html] is a the highest international tribunal that was established to settle disputes related to sport through arbitration. Starting in 2016, an anti-doping division of CAS began judging doping cases at the Olympic Games, replacing the IOC disciplinary commission.

McLaren Report and Russian Athletes Banned

In 2014, Stepanova, a Russian track athlete, and her husband, a former employee of the Russian Anti-Doping Agency, appeared in a documentary [https://presse.wdr.de/plounge/tv/das_erste/2014/12/_pdf/English-Skript.pdf] accusing the Russian sports system of large-scale doping fraud. They indicated that Russian athletics officials supplied banned substances in exchange for 5% of an athlete's earnings and falsified tests together with doping control officers.

In May 2016, Dr. Grigory Rodchenkov [http://www.bbc.com/news/world-europe-36833962] , the former Director of Moscow and Sochi doping control laboratories, further alleged and detailed [http://www.nytimes.com/2016/05/13/sports/russia-doping-sochi-olympics-2014.html?_r=2] widespread efforts facilitated by Russian intelligence services to circumvent positive testing results for Russian athletes. The WADA then engaged Professor Richard McLaren [http://globalnews.ca/news/2831251/russian-doping-report-who-is-richard-mclaren/] to investigate allegations of Russian state manipulation of the doping control process for Russian athletes. On July 18, the results of McLaren's investigation were released in a report [https://www.wada-ama.org/en/resources/doping-control-process/mclaren-independent-investigations-report-into-sochi-allegations] that included findings on Moscow's involvement in circumventing the testing process, including:

> *The State had the ability to transform a positive analytical result into a negative one by ordering that the analytical process of the Moscow Laboratory be altered. The Ministry of Sport ("MofS"), Russian Anti-Doping Agency (RUSADA) and the Russian Federal Security Service (the "FSB") were all involved in this operation.*

> *The MofS directed, controlled and oversaw the manipulation of athletes' analytical results and sample swapping, with the active participation and assistance of the FSB; the Center of Sports Preparation of National Teams of Russia (CSP); and, both Moscow and Sochi laboratories.*

Following the report, the WADA recommended [https://www.wada-ama.org/en/media/news/2016-07/wada-statement-independent-investigation-confirms-russian-state-manipulation-of] that all Russian Olympic and Paralympic athletes be banned from the Rio games. The IOC ultimately cleared 271 of the 389 Olympic athletes for competition and the CAS upheld the ban [http://www.reuters.com/article/us-sport-olympics-doping-idUSKCN101108] while the International Paralympic Committee (IPC) banned the entire Russian Paralympic team from participation.

FANCY BEAR Consistencies

Investigating the two domains provided in the WADA alert [https://m.paralympic.org/news/wada-warns-stakeholders-phishing-scams] -- wada-awa[.]org and wada-arna[.]org -- using SOA and WHOIS records we were able to identify that they were registered by rob_parks@mail[.]com and macie.dietrich50@mail[.]com respectively. Leveraging capabilities from our partners at DomainTools [http://www.domaintools.com/] , we were able to identify that macie.dietrich50@mail[.]com had also registered one other domain -- tas-cass[.]org -- approximately three hours before registering wada-arna[.]org on August 8th. We found no other domains registered by rob_parks@mail[.]com.

```
Domain Name: TAS-CASS.ORG
Domain ID: D189537838-LROR
WHOIS Server:
Referral URL: http://www.PublicDomainRegistry.com
Updated Date: 2016-08-09T07:04:10Z
Creation Date: 2016-08-08T12:17:22Z
Registry Expiry Date: 2017-08-08T12:17:22Z
Sponsoring Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Sponsoring Registrar IANA ID: 303
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibite
d
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibite
d
Registrant ID: DI_59482760
Registrant Name: Macie Dietrich
Registrant Organization: N/A
Registrant Street: Riga
Registrant City: Riga
Registrant State/Province: Rlga
Registrant Postal Code: 24341
Registrant Country: LV
Registrant Phone: +371.2355325313
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: macie.dietrich50@mail.com
```

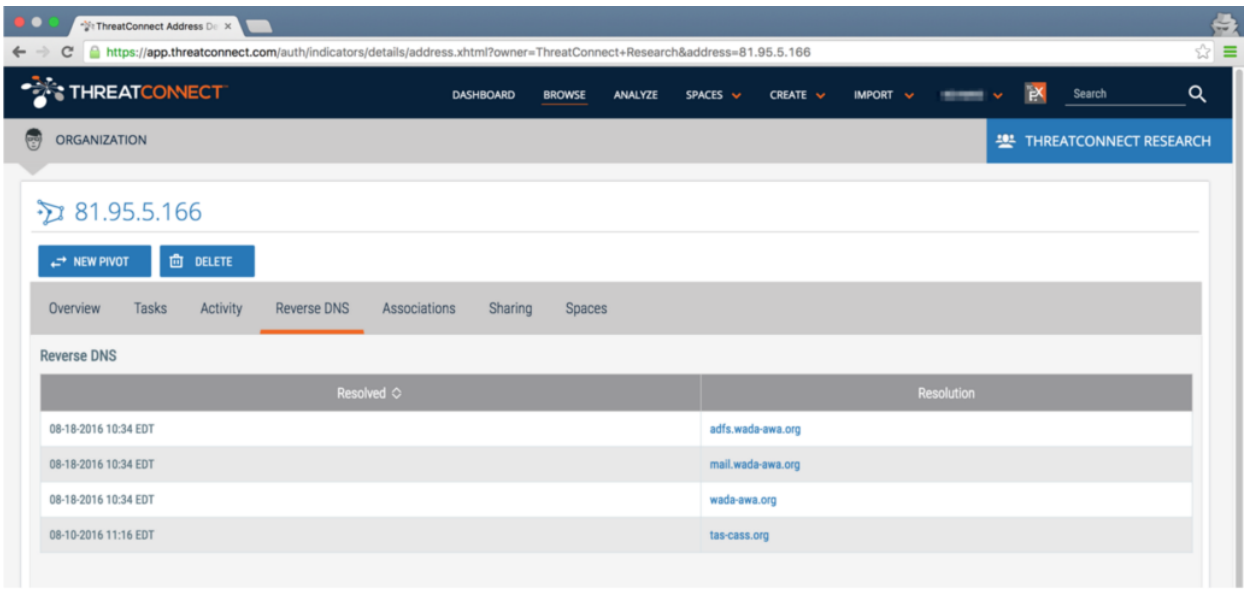
```
Domain Name: WADA-ARNA.ORG
Domain ID: D189539147-LROR
WHOIS Server:
Referral URL: http://www.PublicDomainRegistry.com
Updated Date: 2016-08-09T08:35:58Z
Creation Date: 2016-08-08T15:33:21Z
Registry Expiry Date: 2017-08-08T15:33:21Z
Sponsoring Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Sponsoring Registrar IANA ID: 303
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibite
d
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibite
d
Registrant ID: DI_59482760
Registrant Name: Macie Dietrich
Registrant Organization: N/A
Registrant Street: Riga
Registrant City: Riga
Registrant State/Province: Rlga
Registrant Postal Code: 24341
Registrant Country: LV
Registrant Phone: +371.2355325313
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: macie.dietrich50@mail.com
```

The wada-awa[.]org and tas-cass[.]org domains are currently hosted at the same 81.95.5[.]166 (Germany) IP address with no other domains. While these domains were registered using different email addresses, their hosting at the same IP with no other domains suggests they were registered by the same individual or group. The wada-arna[.]org domain is currently hosted on a dedicated server at 149.154.157[.]171 (Italy).

Based on passive DNS resolutions identified through PassiveTotal [https://www.passivetotal.org/] and our integration with Farsight, [https://www.farsightsecurity.com/] we were able to identify that several subdomains for these domains are currently hosted on these IP

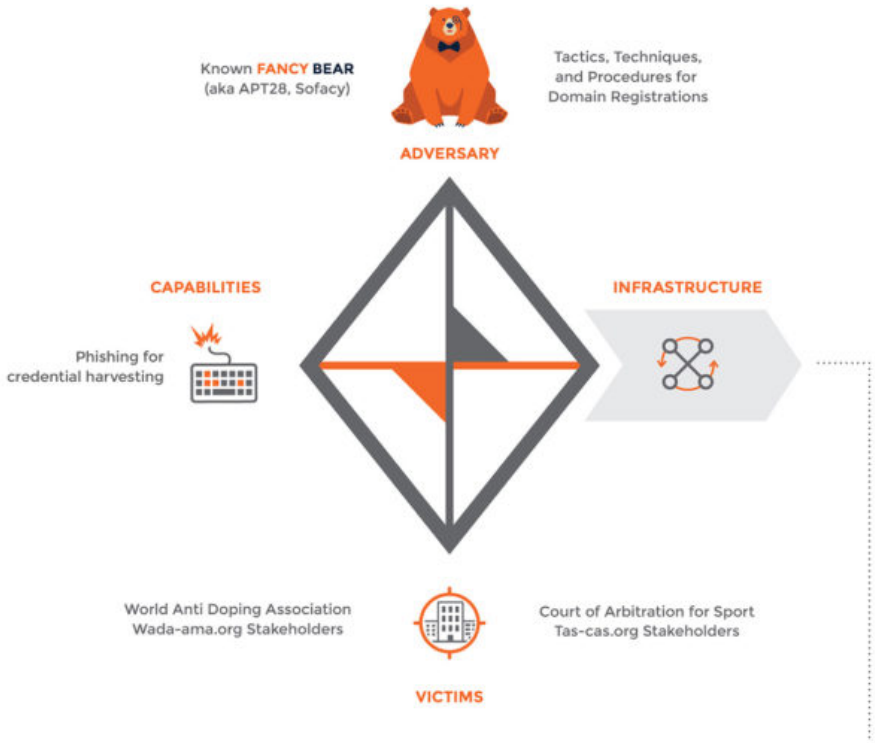
addresses. These subdomains most likely have been used in operations against the WADA and/or CAS:

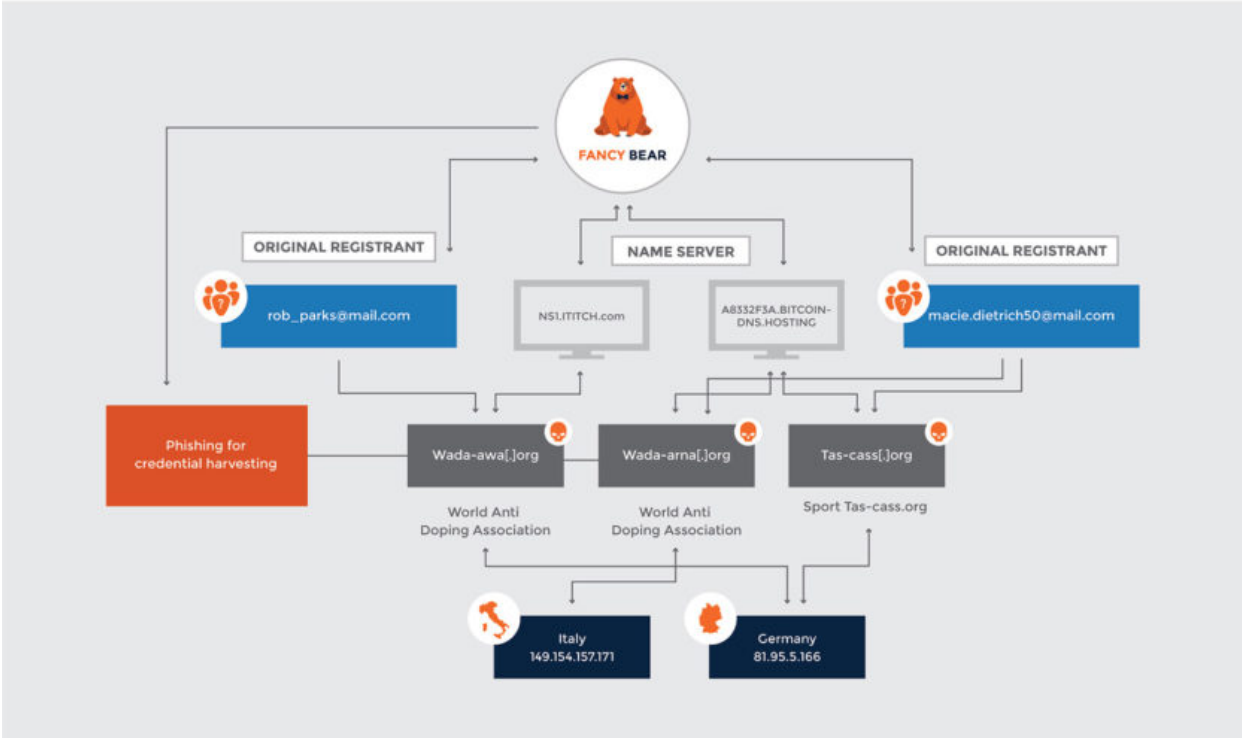
- **mail.wada-awa[.]org**
- **inside.wada-arna[.]org**
- **adfs.wada-awa[.]org**



After taking a look at the name server information for the domains, we identified that wada-awa[.]org was registered and uses a name server from ITitch[.]com, a domain registrar that FANCY BEAR actors recently used to register a domain for operations against the Democratic Congressional Campaign Committee [https://threatconnect.com/blog/fancy-bear-it-itch-they-cant-scratch/] . Wada-arna[.]org and tas-cass[.]org were registered through and use name servers from Domains4bitcoins[.]com, a registrar that has also been associated [https://threatconnect.com/blog/whats-in-a-name-server/] with FANCY BEAR activity. Concentrations of FANCY BEAR domains have been found on the name servers for both of these registrars, and the registrars' acceptance of anonymous Bitcoin payment is desirable for actors seeking to avoid attribution. The diamond model [https://www.threatconnect.com/platform/methodology/] below shows

the relationship between the identified domains, their registration and hosting information, known FANCY BEAR TTPs, and intended targets.





The WADA and CAS-spoofing domains and activity most likely are intended to support Russian government intelligence collection and/or influence operations related to the WADA and CAS. Our assessment is based on the following findings:

1. The registration of these domains on August 3rd and 8th, 2016 are consistent with the timeline in which the WADA recommended banning all Russian athletes from the Olympic and Paralympic games.
2. The use of 1&1 mail.com webmail addresses to register domains matches a TTP we previously identified [https://threatconnect.com/blog/fancy-bear-it-itch-they-cant-scratch/] for FANCY BEAR actors.
3. These domains were registered through ititch[.]com and domains4bitcoins[.]com, two registrars that accept Bitcoins for payments. The use of such registrars also matches an identified [https://threatconnect.com/blog/whats-in-a-name-server/] TTP for FANCY BEAR actors. Two of our previous blog posts also highlighted domains at the ITitch [https://threatconnect.com/blog/fancy-bear-it-itch-they-cant-scratch/] and Domains4bitcoins [https://threatconnect.com/blog/whats-in-a-name-server/] name servers and their associations to FANCY BEAR activity.

A review of recently registered domains using the same name servers identified two other domains related to sports and athletics -- **espn-com[.]co** and **espn-live[.]co**. Espn-live.co was registered through ITitch on August 17. Espn-com[.]co was registered through ITitch on August 2, a day before wada-awa[.]org was registered through the same service. These domains no longer use ITitch name servers as both most likely were taken over by MarkMonitor on ESPN's behalf shortly after they were registered. No information on the original registrants could be identified and we do not have any indication that these domains were used maliciously; however, based on the timing, subject matter, and registrar used, this may represent an additional avenue through which the actors intended to pursue WADA and CAS-related targets.

Anonymous Poland - What's Their Role?

On August 12, 2016 hackread.com [https://www.hackread.com/world-anti-doping-agency-site-hacked/] broke the story that the WADA and CAS had been hacked and thousands of accounts had been leaked. The subtitle for the story read: *Anonymous Poland Hacked World Anti-doping Agency and Court of Arbitration for sport's server' server and leaked personal details for God knows what reason!*

We asked ourselves that very question - what beef does Anonymous Poland (@anpoland [https://twitter.com/anpoland]) have with WADA and CAS? While it is plausible that the attacks were in response to the Tomasz Zielinski being sent home [http://www.reuters.com/article/us-olympics-rio-weightlifting-pole-idUSKCN10K1Y2] for testing positive for a banned steroid nandrolone on August 9, such retaliation efforts are atypical for Anonymous Poland, which has previously focused [https://www.facebook.com/AnonPLorg/] on Polish politics and perceived issues with the financial, political, and media industries. To that end, is it possible that @anpoland is another platform that Russians are using to hide their hand in activity against the WADA and CAS?

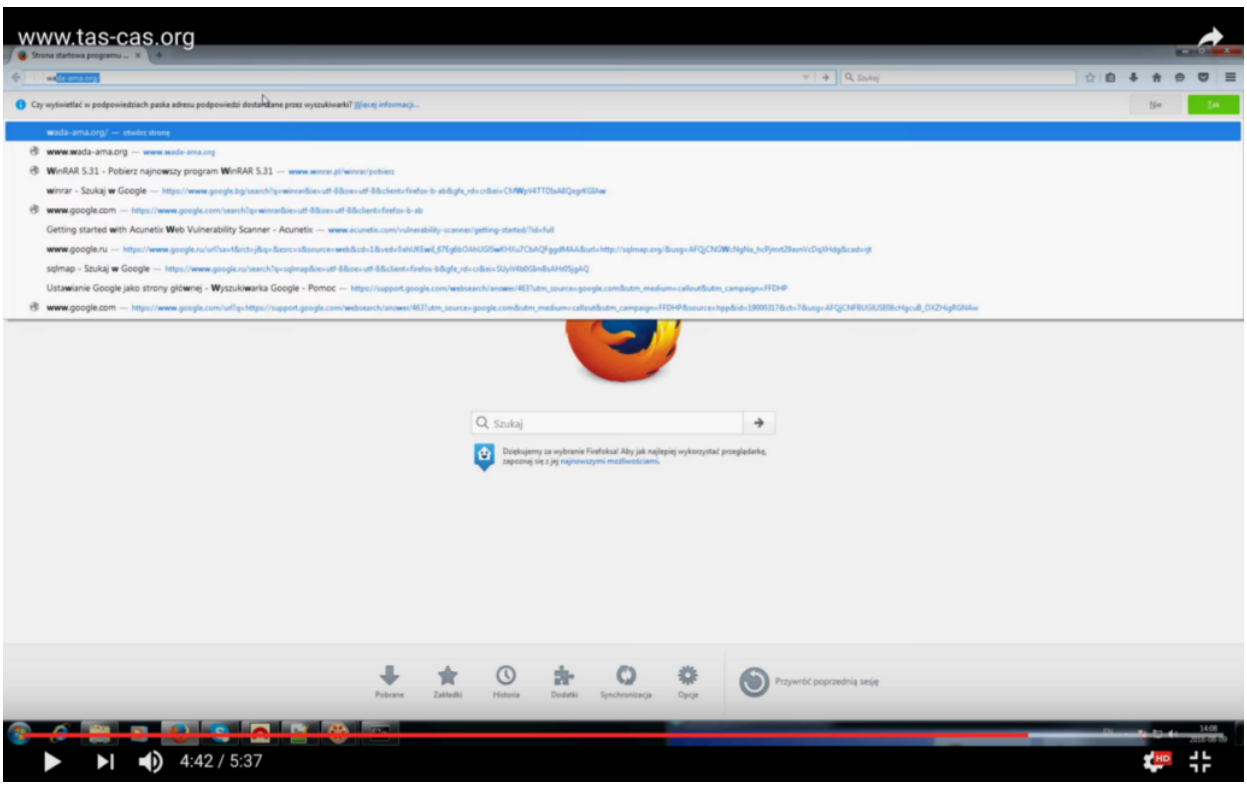
Of course, activity against WADA and CAS from hacktivists and Russian state sponsored actors are not mutually exclusive, so it is entirely possible that two groups could have targeted and/or compromised these organizations at the same time. However, the timing associated with the Russian phishing activity and Anonymous Poland's claims are very coincidental and suggest that the two may be involved. To that end, we reviewed Anonymous Poland's activities to determine whether they are whom they claim to be. Our findings include the following:

1. @anpoland posted a video [https://www.youtube.com/watch?v=day5Aq0bHsA] to Youtube that demonstrates how they purportedly used Acunetix to scan the CAS website and SQLMap

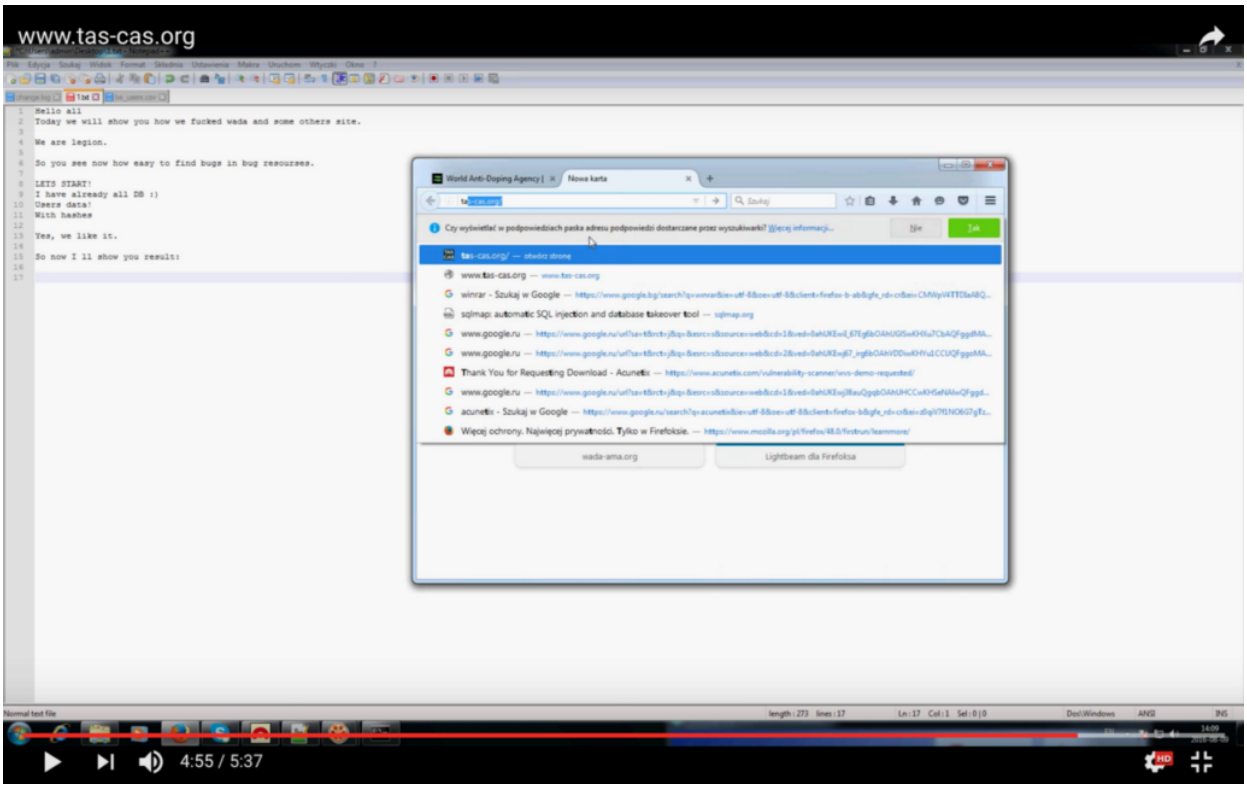
[http://sqlmap.org/] to exploit CAS databases. The screen capture video shows the individual using a local admin account with Polish language settings. However, when the individual uses Firefox, we see in their browser history that they have previously issued Google searches from Google.ru (Russia) and Google.com (US) multiple times while Google.pl (Poland) is absent.

Google.ru within the browser history might indicate that the user that created the Youtube video is originating, or has previously originated, from a Russian IP address. Although the user has Tor browser on their desktop it appears as if they failed to execute it, as it does not appear as an executing process during the hack demo.

WADA Browser History [https://youtu.be/day5Aq0bHsA?t=282]



TAS Browser History [https://www.youtube.com/watch?v=day5Aq0bHsA&feature=youtu.be&t=296]



1. The @anpoland Twitter account being cited by various news outlets as a source for this story, appears to have been inactive until the end of July 2016.
    1. The @anpoland account was established in April 2010, the same timeframe as when Polish Air Force Flight 101 [https://en.wikipedia.org/wiki/2010_Polish_Air_Force_Tu-154_crash] crashed several hundred meters short of the Smolensk airport runway in dense fog, killing everyone on board, including Polish President Kaczyński. Russia's final report on the incident blamed the late president and his "inebriated" air force commander-in-chief for the accident.
    2. Beginning on August 1, the @anpoland account essentially resurfaced with claims that it had hacked the Ukrainian Ministry of Internal Affairs and released hacked documents pertaining at gmarine.com[.]ua - a Ukrainian website hosted on a Russian IP.
    3. It's important to note that while the @anpoland account has a gap in posts from 2010 to 2016, it is possible the individual(s) running the account deleted older posts.

2. Other social media accounts claiming affiliation with Anonymous Poland, such as @anonpoland [https://twitter.com/anonpoland] , and Anonymous' main twitter account [https://twitter.com/YourAnonNews/] are not publicizing the WADA compromise. The inability to confirm the @anpoland and HackRead story with several additional Anonymous Poland-related sources is suspect.
    1. Anonymous Poland Facebook [https://www.facebook.com/AnonPLorg/] accounts identified to date are focused on internal Polish politics and current events, apart from some posts referencing ISIS, most of the communications released call for action (mostly peaceful physical protests) in response to perceived issues with the financial, political, and media industries in the country.

At this time, based on a lack of sources, we cannot conclude that @anpoland is another platform that Russian actors are using for influence operations. However, mounting circumstantial evidence that negate @anpoland's claimed origins makes us skeptical that they are in fact a legitimate Anonymous hacktivist group.

Fancy Bear's Roid Rage

Ultimately, successful operations against WADA and CAS stakeholders could yield Russia with intelligence that could facilitate the following:

1. Follow-on operations seeking to influence or coerce individuals in key decision-making positions within those organizations. Such influence might ultimately result in decisions from those organizations that benefit Russian athletes.
2. Document or data collection that can be used in influence operations or propaganda derisive to the WADA, CAS, or their

stakeholders.

3. Follow-on operations targeting specific individuals to gain additional collection.
4. Intelligence collection that informs Russian efforts to circumvent doping and testing procedures, like those described in the McLaren Report.
5. Publicly intimidate other potential whistleblowers and deter them from coming forward.

As evidenced in the Stepanova compromise [https://www.wada-ama.org/en/media/news/2016-08/wada-confirms-illegal-activity-on-yuliya-stepanovas-adams-account] , we would also expect to see additional Russian cyber operations targeting Professor McLaren and the main source of the investigation, Dr. Rodchenkov. Collection against these individuals could also facilitate Russian efforts like those previously listed, or effort to conduct influence operations that privately intimidate or publicly cast those individuals in a negative light.

Russian activity targeting these organizations is an important example of how Russia responds to wide-reaching current events that have negative implications for Moscow. Organizations involved in such events can reasonably expect to experience targeted Russian cyber operations that ultimately facilitate retaliatory influence or propaganda efforts against them. Knowledge of this TTP, and others associated with Russian APT activity, can help those organizations augment their security posture and defend against such retaliation.

ThreatConnect would very much like to work with WADA and Yuliya Stepanova if either would be open to sharing any details to help us better understand the details surrounding this event feel free to contact us.

Read the full series of ThreatConnect posts following the DNC Breach: "Rebooting Watergate: Tapping into the Democratic National

Committee [https://www.threatconnect.com/tapping-into-democratic-national-committee/] ", "Shiny Object? Guccifer 2.0 and the DNC Breach [https://www.threatconnect.com/guccifer-2-0-dnc-breach/] ", "What's in a Name Server? [https://www.threatconnect.com/whats-in-a-name-server/] ", "Guccifer 2.0: the Man, the Myth, the Legend? [https://www.threatconnect.com/reassesing-guccifer-2-0-recent-claims/] ", "Guccifer 2.0: All Roads Lead to Russia [https://www.threatconnect.com/guccifer-2-all-roads-lead-russia/] ", "FANCY BEAR Has an (IT) Itch that They Can't Scratch [https://www.threatconnect.com/fancy-bear-it-itch-they-cant-scratch/] ", "Does a BEAR Leak in the Woods? [https://www.threatconnect.com/blog/does-a-bear-leak-in-the-woods/] ", "Russian Cyber Operations on Steroids [https://www.threatconnect.com/blog/fancy-bear-anti-doping-agency-phishing/] ", and "Can a BEAR Fit Down a Rabbit Hole? [https://www.threatconnect.com/blog/state-board-election-rabbit-hole/] ".

Categories: Blog , Featured Article , Threat Research

ABOUT THE AUTHOR

The ThreatConnect Research Team: is an elite group of globally-acknowledged cybersecurity experts, dedicated to tracking down existing and emerging cyber threats. We scrutinize trends, technology and socio-political motivators to develop comprehensive knowledge of the cyber landscape. Then, we share what we've learned so that you can protect your organization, and your team can take precise action against threats.