

Email Investigation

Scenario: In this exercise, you have been given a compromised device. During your investigation, you have isolated an email address as the source of the compromise.

Goal: You are tasked with investigating the email address to gain more information about the threat actor.

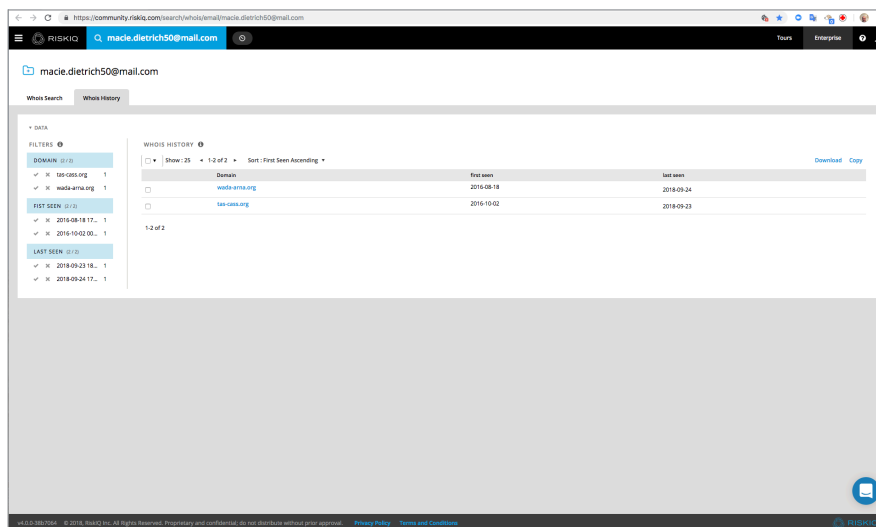
Objective 1: What have you determined about this email address?

Objective 2: Is there any threat actor associated with the email address?

Objective 3: What have you discovered about this threat actor?

STEP 1: Perform a search for macie.dietrich50@mail.com

<https://community.riskiq.com/search/whois/email/macie.dietrich50@mail.com>

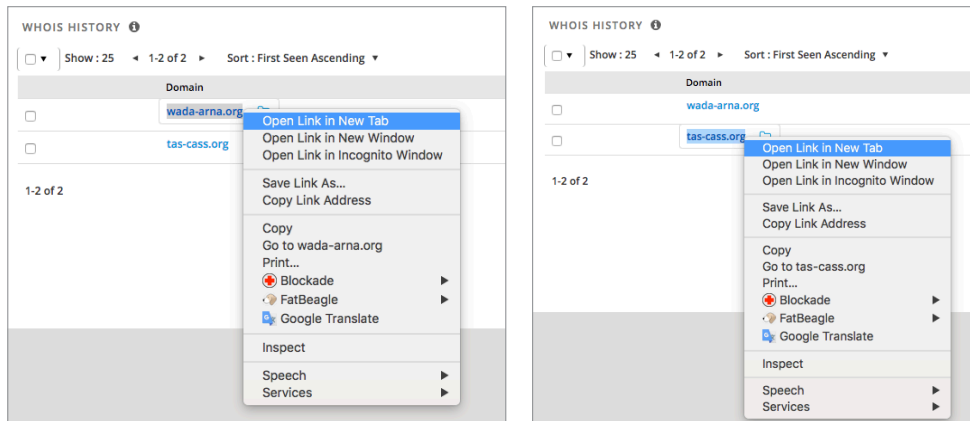


The screenshot shows the RiskIQ search results for the email address macie.dietrich50@mail.com. The page displays a 'WHOIS HISTORY' table with two entries. The first entry is for the domain wade-ortho.org, which was first seen on 2018-08-18 and last seen on 2018-09-24. The second entry is for the domain tan-cats.org, which was first seen on 2018-10-02 and last seen on 2018-09-23. The table is sorted by 'First Seen' in ascending order. The page also includes a 'FILTERS' section on the left with options for 'DOMAIN', 'FIRST SEEN', and 'LAST SEEN'. The footer of the page contains the RiskIQ logo and a 'Privacy Policy' link.

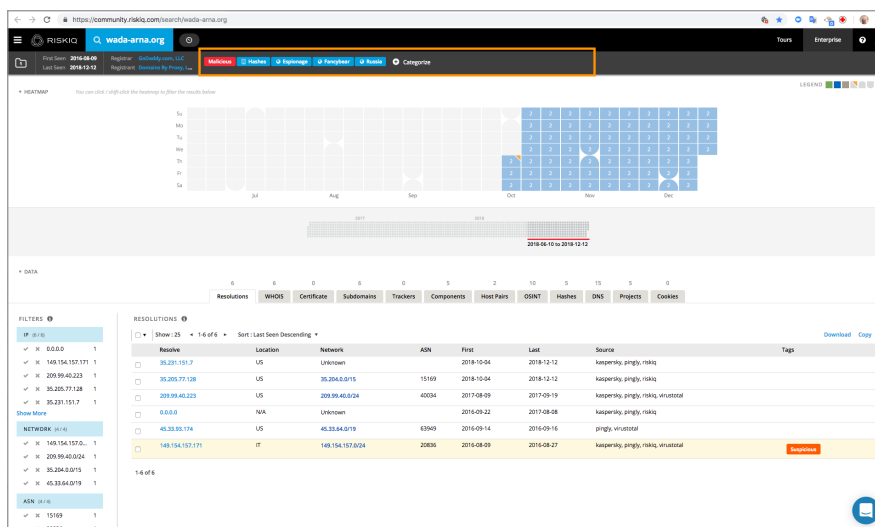
Domain	first seen	last seen
wade-ortho.org	2018-08-18	2018-09-24
tan-cats.org	2018-10-02	2018-09-23

From the WHOIS history, we see that two domains were registered using macie.dietrich50@mail.com.

Step 2: wada-arna[.]org and tas-cass[.]org in a new tab.

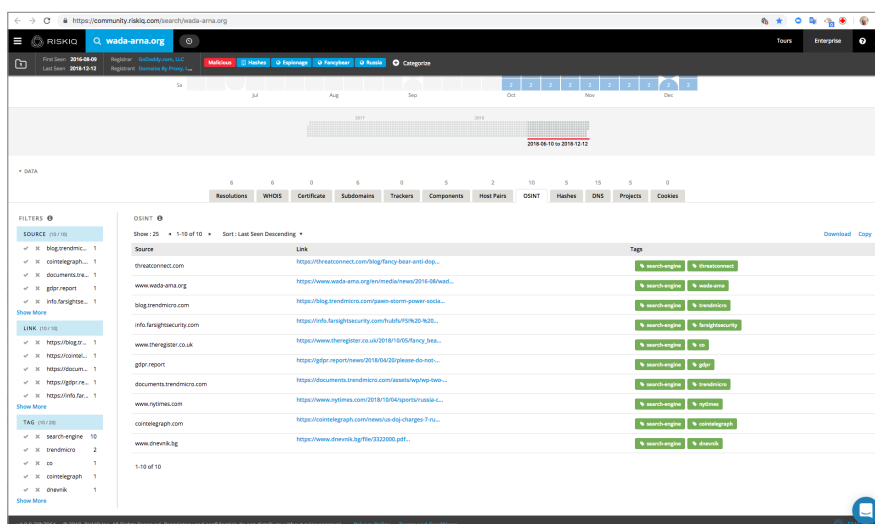


Step 3: Go to the tab for wada-arna[.]org



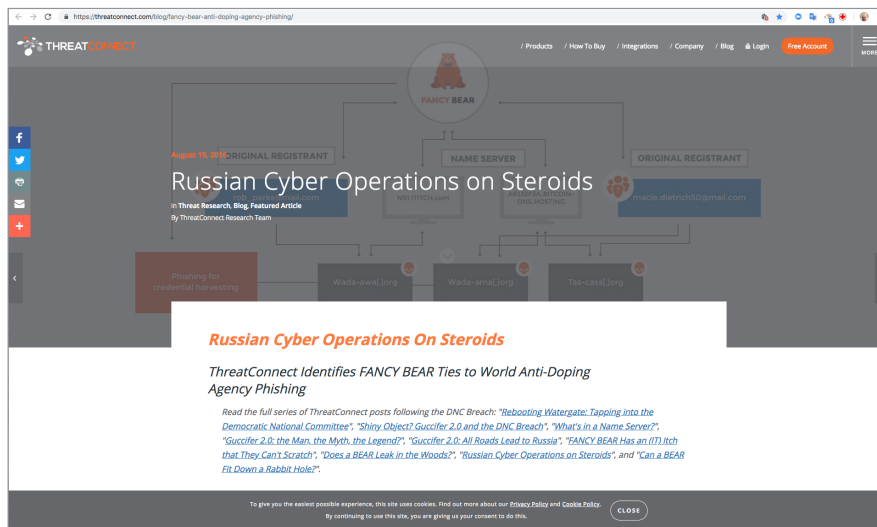
We can see the domain has been flagged as “Malicious,” “Espionage,” “Fancy Bear,” and “Russia.”

Review the open source intelligence tab (OSINT).



Step 4: Click on the link from threatconnect.

<https://threatconnect.com/blog/fancy-bear-anti-dop...>

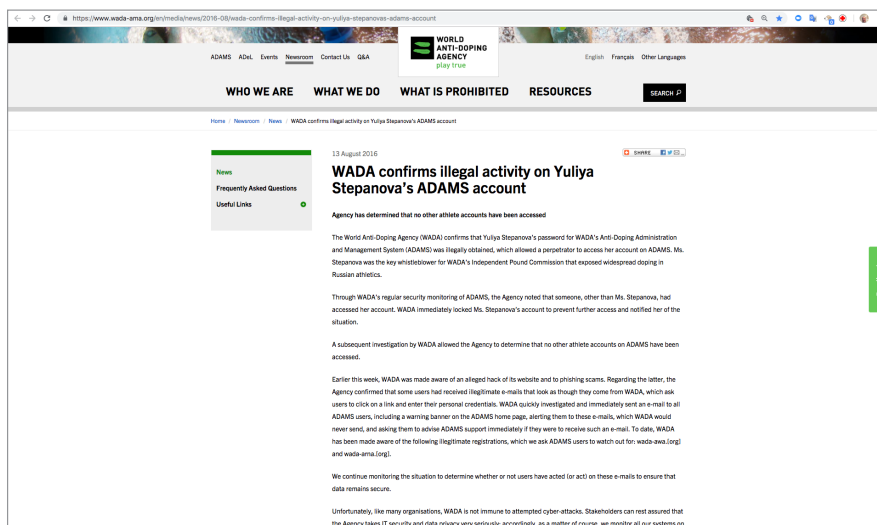


Objective 1: What have you determined about this email address?

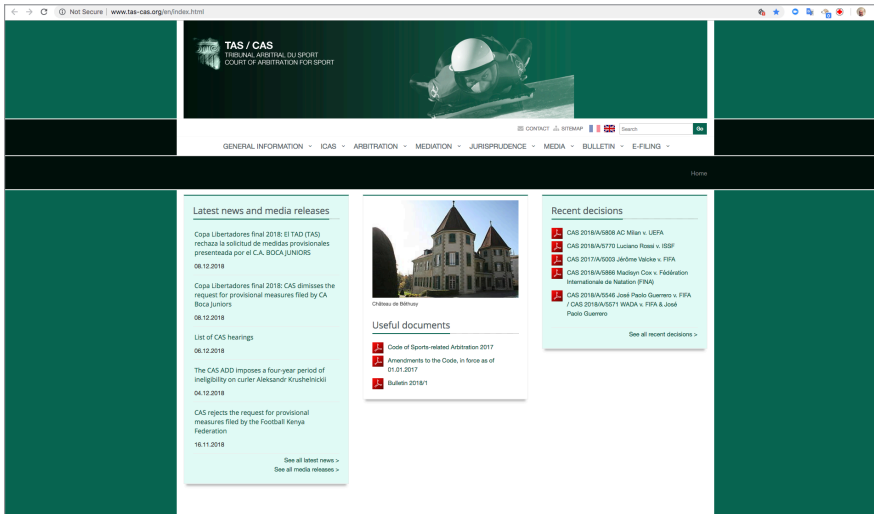
Objective 2: Is there any threat actor associated with the email address?

We have determined that macie.dietrich50@mail.com is associated with two separate domains: wada-arna[.]org and tas-cass[.]org. Through your investigation of a single email address, macie.dietrich50@mail.com, you identified that it was related to wada-arna.org, a confirmed malicious domain. By examining the open source intelligence (OSINT) on this domain, you learned that the wada-arna.org domain was associated with Fancy Bear, a Russian threat actor who targeting the World Anti-Doping Agency Phishing Attack.

Wada-arna[.]org is a typosquatted domain for wada-ama.org, the world Anti-Doping Agency.



Tas-cass[.]org is a typosquatted domain for tas-cas.org, the Tribunal Arbitral Du Sport also called the Court of Arbitration for sports.



Objective 3: What have you discovered about this threat actor?

The United States District Court Western District of Pennsylvania issued an indictment for the Russian Federation Intelligence Directorate of General Staff (GRU) for this particular attack. You can read the indictment at the following URL: <https://www.justice.gov/opa/page/file/1098481/download>

Case 2:18-cr-00263-MRH Document 4 Filed 10/03/18 Page 1 of 41

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA

v.

ALEKSEI SERGEYEVICH MORENETS
EVGENII MIKHAYLOVICH SEREBRIAKOV
IVAN SERGEYEVICH YERMAKOV
ARTEM ANDREYEVICH MALYSHEV
DMITRIY SERGEYEVICH BADIN
OLEG MIKHAYLOVICH SOTNIKOV
ALEXEY VALEREVICH MININ

Defendants.

Criminal No. 18-263

18 U.S.C. §§ 371, 1030(a)(2)(C),
1030(a)(5)(A)
(Conspiracy)
18 U.S.C. § 1349 and § 3559(g)(1)
(Conspiracy to Commit Wire Fraud)
18 U.S.C. § 1343 (Wire Fraud)
18 U.S.C. § 1028A
(Aggravated Identity Theft)
18 U.S.C. § 1956(h)
(Conspiracy to Launder Money)

[UNDER SEAL]

INDICTMENT

COUNT ONE
(Conspiracy)

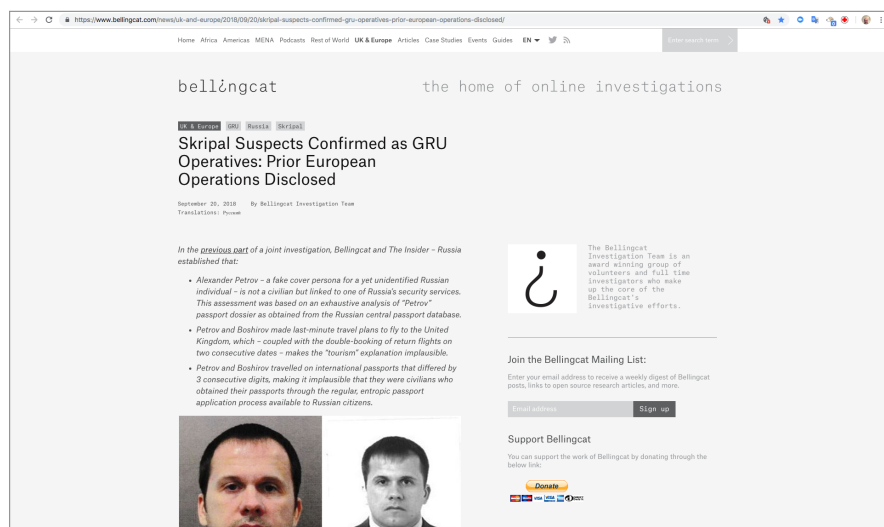
The grand jury charges:

1. At all times relevant to the indictment, from at least 2014 up to and including May 2018, the Russian Federation (Russia) operated a military intelligence agency called the Main Intelligence Directorate of the General Staff (GRU). The GRU was headquartered in Moscow, Russia, and was comprised of multiple units, including Units 26165 and 74455. Military Unit 26165, also known as the "GRU 85 Main Special Service Center," was located at 20 Komsomolskiy Prospekt, Moscow, Russia. Military Unit 74455 was located at 22 Kirova Street, Khimki, Moscow, Russia.

1

FILED
OCT 03 2018
CLERK U.S. DISTRICT COURT
WEST. DIST. OF PENNSYLVANIA

Further information about the FancyBear threat actor group links them to the GRU at Bellingcat. You can read the report at the following url: <https://www.bellingcat.com/news/uk-and-europe/2018/09/20/skrpal-suspects-confirmed-gru-operatives-prior-european-operations-disclosed/>



Conclusion:

You might need to use open source intelligence to help in your investigations. In this particular case finding this email address on a compromised host means that you might be dealing with a nation state threat actor. It is important to fully investigate all avenues to fully understand the scope and nature of the attack.



RiskIQ, Inc.
22 Battery Street, 10th Floor
San Francisco, CA. 94111

✉ sales@riskiq.net

☎ 1 888.415.4447

Learn more at [riskiq.com](https://www.riskiq.com)

Copyright © 2020 RiskIQ, Inc. RiskIQ, the RiskIQ logo and RiskIQ family of marks are registered trademarks or trademarks of RiskIQ, Inc. in the United States and other countries. Other trademarks mentioned herein may be trademarks of RiskIQ or other companies.01_20