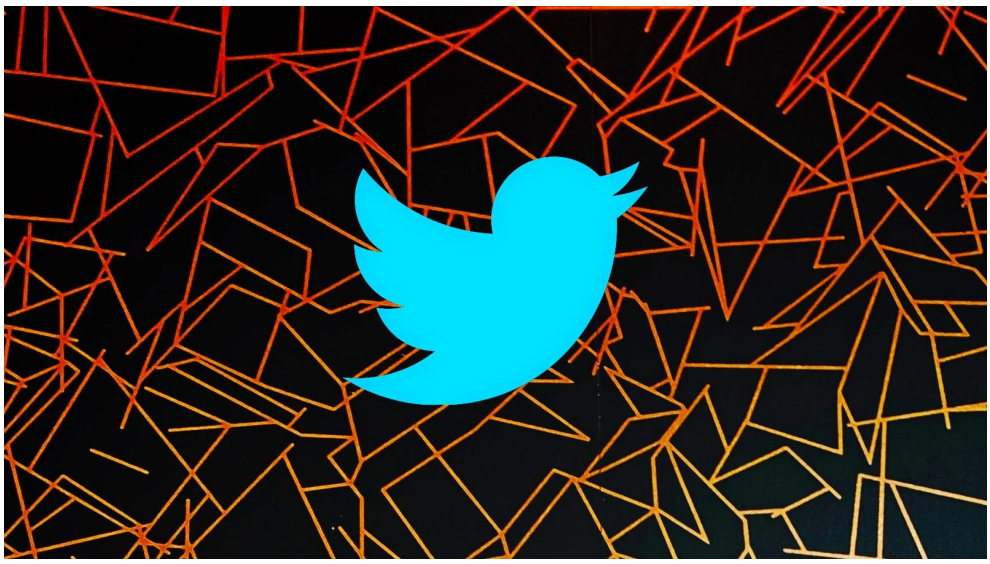
Reality Winner's Twitter account was hacked to target journalists

By **Ax Sharma (https://www.bleepingcomputer.com/author/ax-sharma/)** March 1, 2022 05:46 AM **0**



Twitter account of former intelligence specialist, Reality Winner was hacked over the weekend by threat actors looking to target journalists at prominent media organizations.

Hackers took over Winner's verified Twitter account and changed the profile name to "Feedback Team" to impersonate Twitter staff before sending out suspicious DMs to verified users.

Bogus 'Copyright Infringement' notices

On Sunday, multiple journalists and verified Twitter users reported receiving suspicious DMs from a "verified" Twitter account called "Feedback Team."

On taking a closer look at "Feedback Team's" account's handle *@reazlepuff* however, Jacob Silverman, staff reporter for *The New Republic* pointed out the hacked account appeared to belong to Reality Winner:

> *Pretty sure that this is Reality Winner's account and that it's been hacked. Second image is a DM I just received. pic.twitter.com/KxXZmGfL6B (https://t.co/KxXZmGfL6B)*
>
> *— Jacob Silverman (@SilvermanJacob) February 27, 2022 (https://twitter.com/SilvermanJacob/status/1498005175486885889?ref_src=twsrc%5Etfw)*

Reality Leigh Winner is an American former intelligence specialist who, in 2018, was sentenced to five years and three months in prison for unauthorized release of classified information to the media.

In 2017, Winner shared a National Security Agency (NSA) report about the Russian interference in the 2016 U.S. elections with the news outlet *The Intercept*. The report suggested that Russian hackers had illegally accessed U.S. voter registration rolls via email phishing attacks, although it didn't conclude if this had led to any tampering of electoral records.

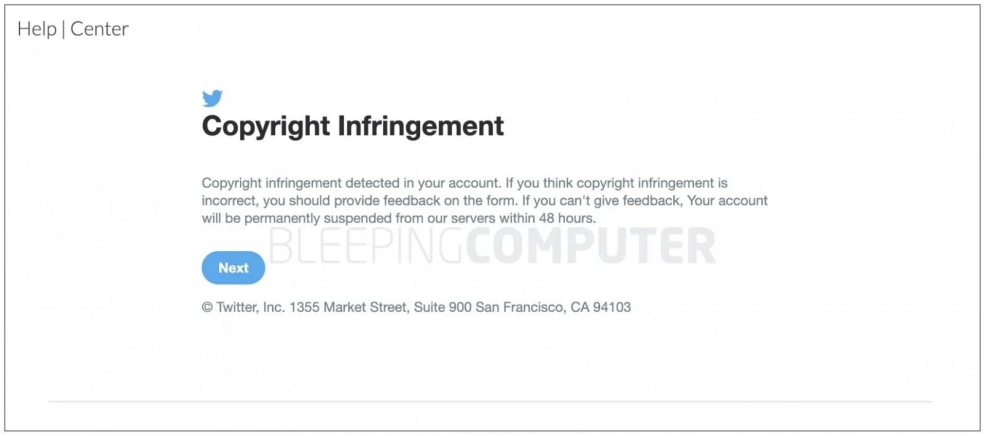
Within minutes of Silverman's tweet, *Daily Dot* staff writer Mikael Thalen also reported (https://twitter.com/MikaelThalen/status/1498005765243564033) receiving the DM, as did writer Tara Dublin (https://twitter.com/taradublinrocks/status/1498008257868156930).

These DMs impersonated Twitter staff and contained bogus "copyright infringement" notices enticing the recipients to click on a Google Sites link.

> Hi Dear User,
>
> Copyright infringement was detected in one of the shares on your account. If you think copyright infringement is wrong, you need to provide feedback. Otherwise, your account will be removed within 48 hours. You can give feedback at the link below. Thank you for your understanding.
>
> https://sites.google.com/view/...
>
> Thanks,
> Twitter Support

The Google Sites webpage, seen by BleepingComputer, contained an embedded HTML iframe.

The contents of the iframe impersonated Twitter's look and feel and asked the user to provide "feedback on the form" to prevent their account from getting "permanently suspended" over copyright infringement:



Phishing webpage embedded on a Google Sites page (BleepingComputer)

The source URL of the malicious iframe, *https://begetadmadir[.]tk/juri/* is no longer accessible, as confirmed by BleepingComputer.

Credentials harvesting attack targets media companies

This appears to be a credentials harvesting attack and this isn't the first time such an attack has occurred either.

Mid-February some Indian journalists, including Sreedevi Jayarajan of *The News Minute* had their verified Twitter account (https://twitter.com/Arv_Ind_Chauhan/status/1493259894656409602) taken over to target other verified profiles in a similar fashion.

The use of the account profile name "Feedback Team," and the identical wording of the DMs sent at the time from Jayarajan's hacked account imply the same threat actor(s) may be behind these attacks.

In January, British actor, comedian, and BBC presenter, Adil Ray "almost fell for this (http://twitter.com/adilray/status/1485346072419573761)" phishing scam purportedly sent by another hacked verified account.

BleepingComputer has previously reported threat actors sending fake DMCA and DDoS complaints (https://www.bleepingcomputer.com/news/security/fake-dmca-and-ddos-complaints-lead-to-bazaloader-malware/) to prominent Twitter accounts to spread malware. This scam, however, distinctly targets media personalities via phishing, to harvest credentials from journalists, with the possible goal of breaching news outlets.

BleepingComputer reached out to Reality Winner to better understand what had happened:

"It started with these log ins from Turkey and I couldn't secure my account quickly enough," Winner tells BleepingComputer.

"I only had a verified account for like 6 days and thought I was gonna lose it. Also I'm really embarrassed that it sent the DM out to journalists, like I felt like I'd lost all credibility."

Additionally, Winner also released a statement (https://twitter.com/reazlepuff/status/1498039537024606214) confirming the hack and expressed regret for anyone affected.

Should you come across a suspicious DM or a Twitter account that appears to be hacked, consider reaching out to real Twitter Support (https://help.twitter.com/en/safety-and-security/twitter-account-hacked).