


# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:48:11 UTC



## ↪ Other threat group: OurMine

Names	OurMine ( <i>real name</i> ) ATK 128 ( <i>Thales</i> ) TAG-HA10 ( <i>Recorded Future</i> )
Country	 <a href="#">Saudi Arabia</a>
Motivation	<a href="#">Financial gain</a>
First seen	2016
Description	<p>OurMine is known for celebrity internet accounts, often causing cyber vandalism, to advertise their commercial services.</p> <p><a href="#">(Trend Micro)</a> In light of the recent report detailing its willingness to pay US\$250,000 in exchange for the 1.5 terabytes’ worth of data swiped by hackers from its servers, HBO finds itself dealing with yet another security breach.</p> <p>Known for hijacking prominent social media accounts, the self-styled white hat hacking group OurMine took over a number of verified Twitter and Facebook accounts belonging to the cable network. These include accounts for HBO shows, such as “Game of Thrones,” “Girls,” and “Ballers.”</p> <p>This is not the first time that OurMine has claimed responsibility for hacking high-profile social networking accounts. Last year, the group victimized Marvel, The New York Times, and even the heads of some of the biggest technology companies in the world. Mark Zuckerberg, Jack Dorsey, Sundar Pichai, and Daniel Ek — the CEOs of Facebook, Twitter, Google and Spotify, respectively — have also fallen victim to the hackers, dispelling the notion that a career in software and technology exempts one from being compromised.</p>

Observed	Sectors: <a href="#">Casinos and Gambling</a> , <a href="#">High-Tech</a> , <a href="#">Media</a> , <a href="#">Telecommunications</a> . Countries: <a href="#">UK</a> , <a href="#">USA</a> .	
Tools used		
Operations performed	Oct 2016	BuzzFeed hacked by OurMine after it claimed to unmask one of its members < <a href="https://www.theguardian.com/technology/2016/oct/05/buzzfeed-hack-ourmine-ahmad-makki-facebook-google">https://www.theguardian.com/technology/2016/oct/05/buzzfeed-hack-ourmine-ahmad-makki-facebook-google</a> >
	Dec 2016	Breach of Netflix and Marvel Twitter accounts < <a href="https://techcrunch.com/2016/12/21/ourmine-hacks-netflixs-u-s-twitter-account/">https://techcrunch.com/2016/12/21/ourmine-hacks-netflixs-u-s-twitter-account/</a> >
	Dec 2016	Breach of Nat Geo Photography's Twitter account < <a href="https://www.hackread.com/ourmine-hacks-nat-geo-photography-twitter-account/">https://www.hackread.com/ourmine-hacks-nat-geo-photography-twitter-account/</a> >
	Jan 2017	Breach of several Twitter accounts affiliated with WWE, including those of WWE Universe, WWE NXT, wrestler and celebrity John Cena, WrestleMania, WWE Network and Summer Slam < <a href="https://mashable.com/2017/01/29/wwe-accounts-twitter-hack-ourmine/">https://mashable.com/2017/01/29/wwe-accounts-twitter-hack-ourmine/</a> >
	Apr 2017	Breach of several Medium blogs < <a href="https://fortune.com/2017/04/27/medium-ourmine-hack/">https://fortune.com/2017/04/27/medium-ourmine-hack/</a> >
	Aug 2017	Game of Thrones secrets revealed as HBO Twitter accounts hacked < <a href="https://www.theguardian.com/media/2017/aug/17/game-of-thrones-secrets-revealed-as-hbo-twitter-accounts-hacked">https://www.theguardian.com/media/2017/aug/17/game-of-thrones-secrets-revealed-as-hbo-twitter-accounts-hacked</a> >
	Aug 2017	Breach of VEVO Vevo, the joint venture between Universal Music Group, Sony Music Entertainment, Abu Dhabi Media, Warner Music Group, and Alphabet Inc. (Google's parent company), was just hacked. Roughly 3.12TB worth of internal files have been posted online, and a couple of the documents reviewed by Gizmodo appear sensitive. < <a href="https://gizmodo.com/welp-vevo-just-got-hacked-1813390834">https://gizmodo.com/welp-vevo-just-got-hacked-1813390834</a> >
	Aug 2017	Breach of PlayStation social media accounts < <a href="https://www.welivesecurity.com/2017/08/21/hackers-target-playstation/">https://www.welivesecurity.com/2017/08/21/hackers-target-playstation/</a> >
	Aug 2017	Breach of Twitter accounts of FC Barcelona and Real Madrid < <a href="https://www.welivesecurity.com/2017/08/28/hacking-group-spanish-giants/">https://www.welivesecurity.com/2017/08/28/hacking-group-spanish-giants/</a> >

	Sep 2017	Breach of DNS records of WikiLeaks < <a href="https://www.grahamcluley.com/despite-appearances-wikileaks-wasnt-hacked/">https://www.grahamcluley.com/despite-appearances-wikileaks-wasnt-hacked/</a> >
	Jan 2020	OurMine crew hijacks social media accounts for the NFL, the 49ers, Cardinals, Bears, Bills, Broncos, Browns, Bucs, Cowboys, Colts, Chiefs, Eagles, Giants, Packers, Texans, and Vikings. < <a href="https://www.zdnet.com/article/hackers-hijack-twitter-accounts-for-chicago-bears-and-green-bay-packers/">https://www.zdnet.com/article/hackers-hijack-twitter-accounts-for-chicago-bears-and-green-bay-packers/</a> >
	Feb 2020	Breach of Facebook's Twitter, Instragram, Messenger's Twitter and Messenger's Instagram accounts < <a href="https://www.zdnet.com/article/hackers-deface-facebooks-official-twitter-and-instagram-accounts/">https://www.zdnet.com/article/hackers-deface-facebooks-official-twitter-and-instagram-accounts/</a> >
	Feb 2020	Breach of the official Twitter accounts of FC Barcelona, the Olympics and the International Olympic Committee (IOC) < <a href="https://www.welivesecurity.com/2020/02/17/fcbarcelona-twitter-account-hacked-again/">https://www.welivesecurity.com/2020/02/17/fcbarcelona-twitter-account-hacked-again/</a> >
Information		< <a href="https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hbo-twitter-and-facebook-accounts-hacked-by-ourmine">https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hbo-twitter-and-facebook-accounts-hacked-by-ourmine</a> > < <a href="https://en.wikipedia.org/wiki/OurMine">https://en.wikipedia.org/wiki/OurMine</a> >

Last change to this card: 09 December 2021

Download this actor card in [PDF](#) or [JSON](#) format

---

Source: <https://apt.etda.or.th/cgi-bin/showcard.cgi?u=cb1c375a-56b6-433e-98d5-cbc7f57fe71e>