Islamic State Hacking Division

> The topic of this article **may not meet Wikipedia's general notability guideline**. Please help to demonstrate the notability of the topic by citing reliable secondary sources that are independent of the topic and provide significant coverage of it beyond a mere trivial mention. If notability cannot be shown, the article is likely to be merged, redirected, or deleted.
> *Find sources:* "Islamic State Hacking Division" – news · newspapers · books · scholar · JSTOR *(August 2015) (Learn how and when to remove this template message)*

The **Islamic State Hacking Division (ISHD)** or The **United Cyber Caliphate (UCC)** is a merger of several hacker groups self-identifying as the digital army for the **Islamic State of Iraq and Levant (ISIS/ISIL**). The unified organization comprises at least four distinct groups, including the **Ghost Caliphate Section, Sons Caliphate Army (SCA), Caliphate Cyber Army (CCA), and the Kalashnikov E-Security Team.** Other groups potentially involved with the **United Cyber Caliphate** are the Pro-ISIS Media group **Rabitat Al-Ansar (League of Supporters)** and the **Islamic Cyber Army (ICA).**[1] Evidence does not support the direct involvement of the **Islamic State** leadership. It suggests external and independent coordination of Pro-ISIS cyber campaigns under the **United Cyber Caliphate (UCC)** name.[2] Investigations also display alleged links to Russian Intelligence group, **APT28**, using the name as a guise to wage war against western nations.[3][4]

Concerns

The group's actions have included online recruiting, website defacement, social media hacks, denial-of-service attacks, and doxing with 'kill lists.'[5][6][7] The group is classified as low-threat and inexperienced because their history of attacks requires a low level of sophistication and rely on publicly available hacking tools.[8][9]

Experts raised doubts about the source and nature of data from released 'kill lists' containing personal information about U.S. Military personnel claimed stolen from hacked U.S. government servers. There is no evidence that the **United Cyber Caliphate (UCC)** compromised U.S. systems. The data included public, unclassified, and often outdated information about civilians, non-U.S. citizens, and others built from old data breaches or web scraped data.[10][11]

U.S., French, and German intelligence Investigated attacks following the French Television Channel TV5Monde hack and The U.S. CENTCOM Twitter attack. All three countries linked actions by the **United Cyber Caliphate (UCC)** to **APT 28,** a Russian intelligence group.[3][4]

History

The group first emerged in hacking operations against U.S. websites in January 2015 as the **Cyber Caliphate Army (CCA)**.[1] In March 2015, the Islamic State published a "kill list" on a website that included names, ranks, and addresses of 100 U.S. military members.[12]

A pattern of similar attacks emerged after the media coverage. At least 19 individual 'kill lists,' including personal information of American, Canadian, and European citizens released between March 2015 and June 2016.[13] On April 4, 2016, all four groups united as the **United Cyber Caliphate (UCC).**[14]

In June 2016, the Middle East Media Research Institute found and revealed to the media an alleged list of approximately 8,300 people around the world as potential lone-wolf attack targets.[15]

Successful attacks since mid-2014

- Australian airport website defaced.[16]
- French TV5Monde live feed hacked, social media hacked and defaced with the message "Je Suis ISIS".[17] French investigators later discounted this, instead suspecting the involvement of a hacking group, APT28, allegedly linked to the Russian government.[18]
- ISIS hacks Swedish radio station and broadcasts recruitment song [19]
- United States' military database hacked in early August and data pertaining to approximately 1400 personnel posted online.[20]
- Top secret British government emails hacked. The emails pertained to top cabinet ministers. The intrusion was detected by GCHQ.[21]
- February 28, 2016, Caliphate Cyber Army (CCA) carried out the bizarre hack on the website of Solar UK, a company in the historic town of Battle, England. Customers were being diverted to a web page featuring the ISIS logo accompanied by a string of chilling threats. “Fear us,” the page warned. “We are the Islamic Cyber Army”.
- On April 15, 2016 (Friday), Islamic State hackers under the name UCC successfully hacked 20 Australian websites in a coordinated attack on Australian business. Some of the websites redirected to the website containing their content.[22]
- In early April 2017, UCC released a kill list of 8,786 people.[23]
- In mid 2019, Islamic State affiliated hacking group hijacked 150 targeted Twitter handles using an unknown vulnerability.[24]

References

1. ^ ***a*** ***b*** *Alkhouri, Laith (2016). "Hacking for ISIS: The Emergent Cyber Threat Landscape" (PDF). Flashpoint.*

2. ^ Alexander, Audrey (April 2019). "Doxing and Defacements: Examining the Islamic State's Hacking Capabilities". CTC Sentinel. **12** (4) – via Combating Terrorism Center at West Point.
3. ^ a b "False Flags: The Kremlin's Hidden Cyber Hand". Observer. 2016-06-18. Retrieved 2017-09-25.
4. ^ a b "Defense Intelligence Agency Releases Russia Military Power Assessment". Defense Intelligence Agency. Retrieved 2017-09-25.
5. ^ Theodore Schleifer, CNN (18 June 2015). "FBI director: We can't yet limit ISIS on social media - CNNPolitics.com". CNN.
6. ^ Emma Graham-Harrison (12 April 2015). "Could Isis's 'cyber caliphate' unleash a deadly attack on key targets?". the Guardian.
7. ^ "Flashpoint - Cyber Jihadists Dabble in DDoS: Assessing the Threat". Flashpoint. 2017-07-13. Retrieved 2020-12-09.
8. ^ Lamothe, Dan. "U.S. military social media accounts apparently hacked by Islamic State sympathizers". Washington Post. ISSN 0190-8286. Retrieved 2020-12-09.
9. ^ Bernard, Rose (2017-05-04). "These are not the terrorist groups you're looking for: an assessment of the cyber capabilities of Islamic State". Journal of Cyber Policy. **2** (2): 255–265. doi:10.1080/23738871.2017.1334805. ISSN 2373-8871.
10. ^ "Doubts cast on Islamic State's so-called leak of US .mil, .gov passwords". theregister.co.uk.
11. ^ Desk, ICT Cyber (2016). "Case Study – "Killing Lists" – The Evolution of Cyber Terrorism?". Cyber-Terrorism Activities Report No. 16: 34–39.
12. ^ Schmidt, Michael S. (21 March 2015). "ISIS Urges Sympathizers to Kill U.S. Service Members it Identifies on Website". The New York Times. Retrieved 8 December 2020.
13. ^ Arsenault, Adrienne (15 June 2016). "ISIS 'kill list' includes names of 151 Canadians". CBC.ca. Retrieved 16 June 2016.
14. ^ "Special Report: Kill Lists from Pro-IS Hacking Groups" (PDF). SITE Intelligence. 2016.
15. ^ "Are you on the Islamic State's kill list? Check here". 10 June 2016. Retrieved 16 June 2016.
16. ^ "Australian airport website hacked by Islamic State". Telegraph.co.uk. 13 April 2015.
17. ^ "Europe - France's TV5Monde targeted in 'IS group cyberattack'". France 24. 9 April 2015.
18. ^ "France probes Russian lead in TV5Monde hacking: sources". Reuters. 10 June 2015. Retrieved 9 July 2015.
19. ^ "Someone Hacked Swedish Radio Station to Play Pro-ISIS Song".
20. ^ Safi, Michael (13 August 2015). "Isis 'hacking division' releases details of 1,400 Americans and urges attacks". the Guardian. Retrieved 2015-08-23.
21. ^ Perry, Keith (11 September 2015). "ISIS hackers intercept top secret British Government emails". Daily Mirror. Retrieved 2015-09-21.
22. ^ "'Are you joking?': Small Australian businesses targeted by pro-IS hackers". ABC News. 15 April 2016.

23. ^ *"ISIS-linked cyber group releases 'kill list' of 8,786 US targets for lone wolf attacks"*. *Newsweek. 2017-04-04. Retrieved 2017-04-09.*
24. ^ *"ACCA Claims Hacking 150 Twitter Accounts | Dark Web and Cyber Security | Articles"*. *ent.siteintelgroup.com. 16 July 2019. Retrieved 2019-07-16.*