AN ANALYSIS OF JIHADI CYBERATTACKS REPORTED IN THE EXTREMIST CYBERCRIME DATABASE (ECCD)

Thomas J. Holt, Steven M. Chermak, Joshua D. Freilich, Noah Turner, and Emily Greene-Colozzi

There were 18 jihadi schemes identified in our data affecting US targets, with the majority of events occurring within the last decade (n=16; see Table 1). In the context of our data, a scheme can involve one or many forms of cyberattack (see Methodology white paper for more detail). As a result, the number of total attacks may be greater than the total number of schemes. To that end, the most schemes occurred in 2015 (n=14; 77.8%). There were 14 incidents affiliated to hacker groups or teams of some type (77.8%). Two were associated to individual hacker handles or nicknames, and the remaining two could not be attributed to any entity. Of the two individuals identified, one was killed during a US military strike due to their involvement with ISIS. The other is currently incarcerated in US federal prison for violations of the Computer Fraud and Abuse Act (CFAA).

Across these 18 schemes, there were 26 total cyberattacks identified in the data, with half of all incidents involving a web defacement (see Table 2). Data breaches (n=5; 19.2%) and doxing incidents (n=5; 19.2%) were also present. Additionally, three unique hacks were observed, mostly involving social media hacks to gain access to Twitter accounts (n=3). The majority of these hacks occurred in 2015 (n=19; 73%), in tandem with some of ISIS's most prolific global growth in on and off-line spaces.

Individuals were impacted in three instances, specifically federal employees whose social media accounts were hacked. In addition, two military entities were affected, including US Strategic Command. Additionally, three government targets were affected: one federal government agency, one state, and one local government. Eight businesses were harmed, as

were five other entities including media groups like Newsweek and a nonprofit group. Seven universities were affected as well, including Harvard University and Stanford University. Additionally, an unknown number of civilian, military, and government affiliated individuals were affected by two data breaches performed by jihadi actors.

Table 1: Jihadi Affiliated Schemes Over Time

	Attacker Affiliation			
Year	Individual	Group	Unknown	Total
2000	0	0	0	0
2001	0	1	0	1
2002	0	0	0	0
2003	0	0	0	0
2004	0	0	0	0
2005	1	0	0	1
2006	0	0	0	0
2007	0	0	0	0
2008	0	0	0	0
2009	0	0	0	0
2010	0	0	0	0
2011	0	0	0	0
2012	0	0	0	0
2013	0	0	0	0
2014	0	1	0	1
2015	1	11	2	14
2016	0	1	0	1
2017	0	0	0	0
2018	0	0	0	0
2019	0	0	0	0
2020	0	0	0	0
Total	2	14	2	18

Table 2: Jihadi Cyberattacks Across Schemes Over Time by Type

	Attack Type						
Year	Data Breach	Data Change	Defacement	DDoS	Doxing	Other	Total
2000	0	0	0	0	0	0	0
2001	0	0	1	0	0	0	1
2002	0	0	0	0	0	0	0
2003	0	0	0	0	0	0	0
2004	0	0	0	0	0	0	0
2005	1	0	1	0	1	1	4
2006	0	0	0	0	0	0	0
2007	0	0	0	0	0	0	0
2008	0	0	0	0	0	0	0
2009	0	0	0	0	0	0	0
2010	0	0	0	0	0	0	0
2011	0	0	0	0	0	0	0
2012	0	0	0	0	0	0	0
2013	0	0	0	0	0	0	0
2014	0	0	1	0	0	0	1
2015	4	0	9	0	4	2	19
2016	0	0	1	0	0	0	1
2017	0	0	0	0	0	0	0
2018	0	0	0	0	0	0	0
2019	0	0	0	0	0	0	0
2020	0	0	0	0	0	0	0
Total	5	0	13	0	5	3	26

Funding

This work was supported by the U.S. Department of Homeland Security [ASUB00000368].