

## **AN ANALYSIS OF FAR LEFT 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 19 schemes identified in our data affecting US targets, with the majority of events occurring within the last decade (n=17; 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 2018 (n=4). There were four incidents linked to Anonymous, two incidents attributed to the ALF, and one to Animal Right Now. Five separate twitter handles were also involved in the schemes. The majority of incidents could not be attributed to an individual or group.

Across these 19 schemes, there were 32 total cyberattacks identified in the data, with only two schemes involving single incidents only (see Table 2). The majority of attacks involved doxing of some form (n=11), followed by data breaches (n=6), defacements (n=6) and DDoS (n=6). There was one incident involving a change of data and two incidents that fall into the category of other. Two of the incidents involving Anonymous featured DDoS attacks, while three involved doxing in keeping with their general attack preferences.

There were 30 distinct entities targeted in these attacks, the majority of which were businesses (n=17). For instance, three separate fur-related businesses and organizations were affected, as were two hunting related entities and a farm. These targets were in line with traditional far-left ideological target selection in physical space. Eight attacks affected individuals, though this could be one person or many depending on the circumstances. For instance, a woman was doxed by Anonymous-affiliated actors for working as a taxidermist and

posing in a photo with a dead tiger's body. In the case of data breaches, multiple victims could be affected simultaneously as when a data breach and doxing affected hundreds of members of a far right group. Only two targeted government resources, one federal and one state.

Additionally, one educational institution was targeted, as was one far right website. Those incidents involving either data breaches or doxing led to a total of 2,853 individual victims who were affected based on reported details.

**Table 1: Far Left Schemes Over Time**

Year	Attacker Affiliation						Total
	ALF	ARN	ANON	ECD	Individual	Unknown	
2005	0	0	0	1	0	0	1
2006	0	0	0	0	0	0	0
2007	1	0	0	0	0	0	1
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	1	0	1	1	3
2012	0	0	0	0	1	2	3
2013	0	0	0	0	0	0	0
2014	0	0	0	0	1	1	2
2015	0	0	2	0	0	0	2
2016	0	0	1	0	1	0	2
2017	0	0	0	0	0	0	0
2018	1	1	0	0	1	1	4
2019	0	0	0	0	0	1	1
<b>Total</b>	<b>2</b>	<b>1</b>	<b>4</b>	<b>1</b>	<b>5</b>	<b>6</b>	<b>19</b>

**Table 2: Far Left Cyberattacks Across Schemes Over Time by Type**

Year	Attack Type						Total
	Data Breach	Data Change	Defacement	DDoS	Doxing	Other	
2005	0	0	0	0	0	1	1
2006	0	0	0	0	0	0	0
2007	0	0	0	1	0	0	1
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	1	1	1	2	2	0	7
2012	2	0	1	1	2	0	6
2013	0	0	0	0	0	0	0
2014	1	0	1	0	1	1	4
2015	0	0	0	1	1	0	2
2016	0	0	0	1	1	0	2
2017	0	0	0	0	0	0	0
2018	1	0	3	0	3	0	7
2019	1	0	0	0	1	0	2
Total	6	1	6	6	11	2	32

**Funding**

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