Profit-motivated cybercriminals disrupted election preparations in some US states with ransomware attacks intended to generate profit. We have no indications that these actors sought to use these attacks to alter election functions or data, nor do we have indications that they were acting on behalf of any government.

- For example, in late October, probably foreign ransomware actors demanded payment from a New York county after encrypting 300 computers and 22 servers on the network with Ragnarok malware that prevented it from connecting to a statewide voter registration system. County officials directed voters who had applied via email for an absentee ballot to call and verify their ballot application had been received and processed.

- We do not know whether cybercriminals specifically targeted election-related networks with profit-making schemes or whether their activity reflected a general targeting of state and local government networks that also happen to host election-related processes.

- We assess foreign cybercriminals probably did not work to interfere or influence the US elections on behalf of or at the direction of a nation state. We have low confidence in this assessment. We assess that some cybercrime groups probably operate with at least the tacit approval of their nation state hosts.

Foreign Hacktivists

The IC tracked a handful of unsuccessful hacktivist attempts to influence or interfere in the 2020 US elections.

- In November, hackers promoting Turkish nationalist themes breached and defaced a website previously established for a candidate in the US presidential campaign, according to US cybersecurity press.

- In October, a hacker briefly defaced a presidential campaign website after gaining access probably using administrative credentials.