THIRD WAY

MEMO *Published April 15, 2020* · *2 minute read*

How Many Ransomware Attacks Have Happened in Your District?

Anisha Hindocha
National Security Fellow
@ThirdWayNatSec

Ishan Mehta
Former Policy Advisor, National Security Program
@ishan_tweeting

Takeaways

- From November 6, 2013 to March 5, 2020, there have been reports of 327 ransomware attacks on public sector entities in the United States, hitting 207 congressional districts. Data tells us that ransomware—when a victims' systems or data are held hostage until a ransom is paid—on both public and private sector entities is increasing.

- There is a lack of consequences imposed on the perpetrators of these attacks in the United States. From June 2014 to December 2019, law enforcement has issued 6 public indictments against perpetrators of ransomware attacks, and only one arrest has been made. This is part of a larger trend. Third Way has found that, on average, only 3 in 1,000 reported cyber incidents, including ransomware, see an arrest.
- Congress has the opportunity to do something about this during the appropriations process. Members of Congress can raise this issue with relevant agency heads and secretaries during the budget hearings and provide more resources to federal agencies to reduce these attacks and bring perpetrators to justice.

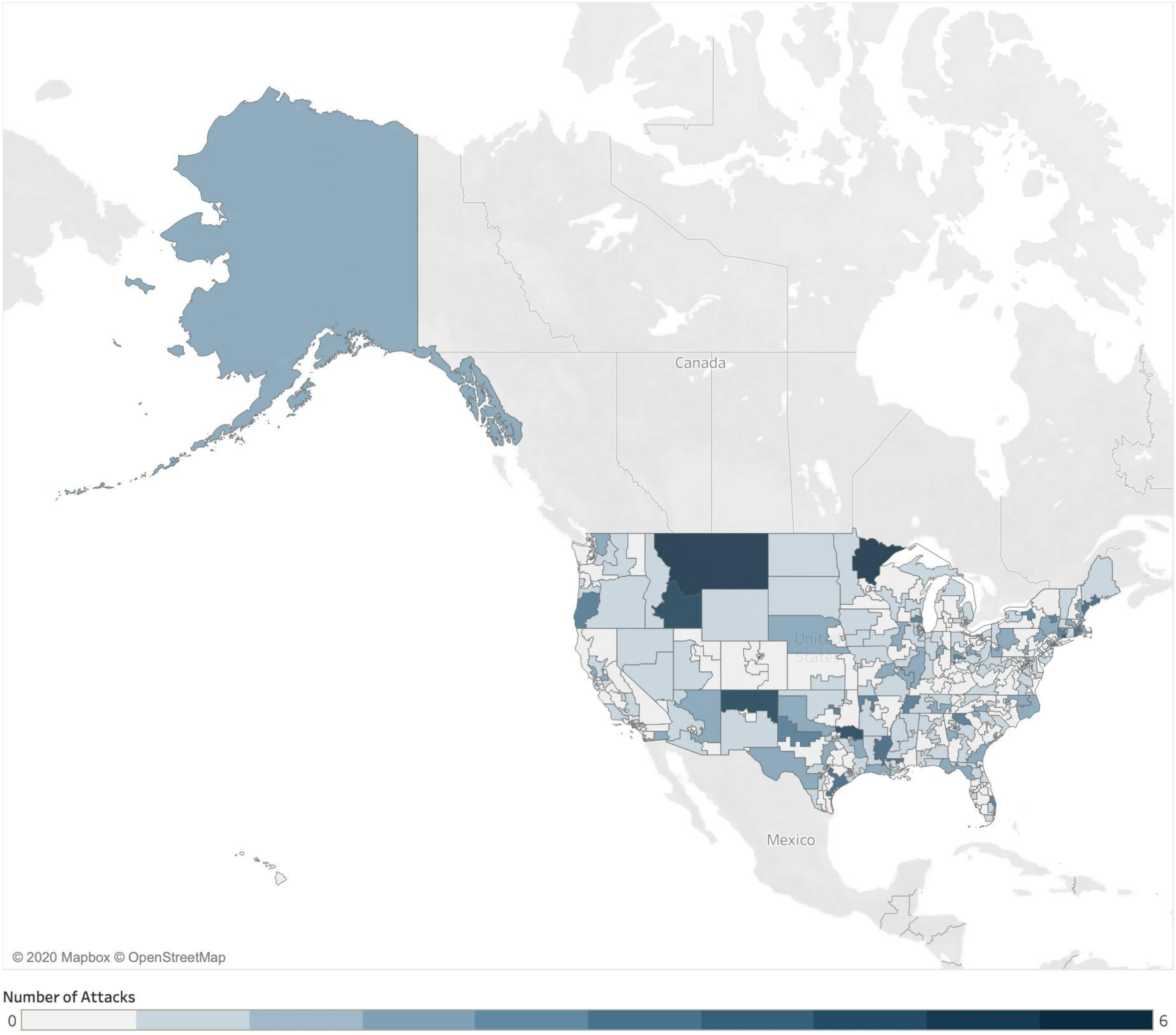
The number of ransomware attacks on the public sector has been steadily increasing since the first reported attack on the Swansea Police Department in Massachusetts in November 2013. [1] Ransomware is a form of malicious software (malware) designed to deny access to a computer system or data until a ransom is paid, usually through encrypting the victim's data. [2] Based on publicly available data gathered by StateScoop, Third Way determined 207 House districts or nearly half of all districts have experienced at least one ransomware attack on a state or local public entity. [3] As of March 5, 2020, there have been 327 reported ransomware attacks since November 2013. Collectively, 44 public entities have paid over $2.6 million in ransom to regain access to their data. Those victims that have not paid ransom have faced tremendous costs in recovery. Texas is the hardest hit state with 30 reported attacks. Particularly worrisome, ransomware poses a particular concern to the public sector during crises such as the current COVID-19 pandemic. [4] For example, the Champaign Urbana Public Health District in Illinois was hit by a strain of ransomware in March, forcing the district to set up an alternate website to provide basic COVID-19 information to the public. [5]

Congress has done little to help law enforcement impose consequences on the human attackers behind these malicious cyber activities. While these ransomware attacks have become more prevalent, law enforcement has not been able to meet the threat. The Department of Justice has issued indictments publicly against perpetrators of 6 strains of ransomware coming from nations like North Korea, Iran, and Russia, but have made only one arrest. [6] More broadly, Third Way has estimated that US law enforcement makes an arrest in less than 1 percent of the total reported malicious cyber incidents occurring per year in the United States. [7]

Congress has an opportunity to do something about the growing threat of ransomware during the appropriations process. Members should take the opportunity to raise this issue with the heads of relevant federal departments and agencies like the Department of Justice, Federal Bureau of Investigation, Department of State, and the Department of Homeland Security. Third Way created the following map to help members of Congress and their staffs find out how many ransomware attacks have happened to a public entity in their districts, if there has been an indictment in each instance, and if an arrest has been made. You can view the spreadsheet on which this data is based on here.

We would like to thank the team at StateScoop, in particular their Technology Editor Benjamin Freed, for collecting the data used in this research for their Ransomware Map. [8]

How Many Public Sector Ransomware Attacks Have Happened in Your District?



Top Hit Districts

District	Number of attacks	Representative
CT-03	5	Rosa DeLauro (D)
ID-02	5	Mike Simpson (R)
NM-03	5	Ben Ray Luján (D)
TX-04	5	John Ratcliffe (R)
MN-08	6	Pete Stauber (R)
MT-at-large	6	Greg Gianforte (R)

TOPICS

CYBERSECURITY 47

ENDNOTES

1. “Ransomware Attacks Map.” *StateScoop*, Scoop News Group, 22 Oct. 2019, https://statescoop.com/ransomware-map/. Accessed 5 Mar. 2020.; Fraga, Brian. “Swansea police pay $750 “ransom” after computer virus strikes.” *The Herald News*, 13 Nov. 2013, https://www.heraldnews.com/x2132756948/Swansea-police-pay-750-ransom-after-computer-virus-strikes. Accessed 16 Mar. 2020.

2. “Ransomware.” CISA, Department of Homeland Security, https://www.us-cert.gov/Ransomware. Accessed 16 Mar. 2020.

3. The data presented in this map is for state and local public sector entities only because comprehensive data for ransomware attacks on the private sector is not readily available. However, in 2019, 205,280 organization has been hacked in a ransomware attack, according to Emisoft, hitting private sectors such as technology, healthcare, manufacturing, financial services, media, and others. Popper, Nathaniel. “Ransomware Attacks Grow, Crippling Cities and Businesses.” *The New York Times*, 9, Feb. 2020. https://www.nytimes.com/2020/02/09/technology/ransomware-attacks.html. Accessed 23 Mar. 2020; “2020 Global Threat Report.” *CrowdStrike*, 3 Mar. 2020, pp. 16, https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf. Accessed 23 Mar. 2020.

4. Peters, Allison and Ishan Mehta. “This is not the time to leave our hospitals unprotected against cyberattacks.” *The Washington Post*, 19 Mar. 2020, https://www.washingtonpost.com/opinions/2020/03/19/this-is-not-time-leave-our-hospitals-unprotected-against-cyberattacks/. Accessed 23 Mar. 2020.

5. Vicens, AJ. “As Coronavirus Spreads, an Illinois Public Health Agency’s Website is Sidelined by Hackers.” Mother Jones, 12 Mar. 2020, https://www.motherjones.com/politics/2020/03/illinois-ransomware-coronavirus/.

6. “U.S. Leads Multi-National Action Against “Gameover Zeus” Botnet and “Cryptolocker” Ransomware, Charges Botnet Administrator.” Press Release, *Department of Justice*, 2 Jun, 2014, https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware. Accessed 5 Mar. 2020; “Two Romanian Suspects Charged With Hacking of Metropolitan Police Department Surveillance Cameras in Connection with Ransomware Scheme.” Press Release, *Department of Justice*, 28 Dec. 2017, https://www.justice.gov/usao-dc/pr/two-romanian-suspects-charged-hacking-metropolitan-police-department-surveillance-cameras. Accessed 5 Mar. 2020; “North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions.” Press Release, *Department of Justice*, 6 Sep. 2018, https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and. Accessed 5 Mar. 2020, “Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses.” Press Release, *Department of Justice*, 28 Nov. 2018, https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public. Accessed 5 Mar. 2020; “Russian National Charged with Decade-Long Series of Hacking and Bank Fraud Offenses Resulting in Tens of Millions in Losses and Second Russian National Charged with Involvement in Deployment of “Bugat” Malware.” Press Release, *Department of Justice*, 5 Dec. 2019, https://www.justice.gov/opa/pr/russian-national-charged-decade-long-series-hacking-and-bank-fraud-offenses-resulting-tens. Accessed 5 Mar. 2020.

7. Eoyang, Mieke, et al. “To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors.” Third Way, *Third Way*, 29 Oct. 2018, pp. 1-2. https://thirdway.imgix.net/pdfs/override/To_Catch_Hacker_Report_FINAL.pdf. Accessed 16 Mar. 2020.

8. “Ransomware Attacks Map.” *StateScoop*, Scoop News Group, 22 Oct. 2019, https://statescoop.com/ransomware-map/. Accessed 05 Mar. 2020.