

Early Findings: Review of State and Local Government Ransomware Attacks

By Allan Liska

Author's Note: The cutoff for this report was the end of April, 2019. Since then, there have been at least three new ransomware attacks against state and local governments: [Lynn](#), Massachusetts, and [Cartersville](#), Georgia, as well as [Baltimore](#), Maryland, which was hit for at least a second time. Unfortunately, ransomware attacks against state and local governments are not going away anytime soon.

2019 marks the 30-year anniversary of the first ransomware attack. [PC Cyborg](#) (also known as the AIDS Trojan because it targeted AIDS researchers) was clunky and required mailing a physical check to an address in Panama. However, modern ransomware — the kind that most people think of today with Bitcoin demands and threats to have all your files deleted — started in 2013 with ransomware variants like [CryptoLocker](#).

State and local governments were among the first organizations to be hit with ransomware. The first known case was in November 2013, when the Swansea Police Department in Massachusetts was infected with [CryptoLocker](#). There may have been more infections, but ransomware was not a commonly used term in 2013 (see the Kaspersky [definition of CryptoLocker](#) as a “virus”), and any earlier attacks may not have been reported as such.

Since then, there has been a lot of [discussion](#) around ransomware attacks [targeting](#) state and local governments, and the attacks have seemingly continued to grow over the years. But I wanted to understand the nature of these attacks and determine whether ransomware is really on the rise in the state and local government sector. To that end, building on the excellent research done by the team at [SecuLore](#) through the Recorded Future data set, and

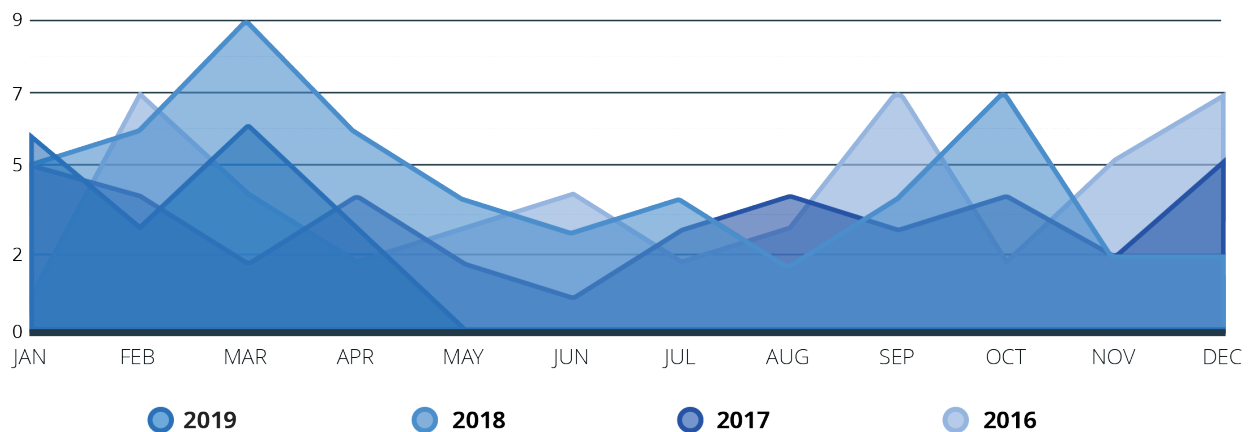
searching through local news sources, I was able to catalog 169 ransomware incidents affecting state and local governments since 2013. This report is a discussion of the findings and trends.

It should be noted that this list should not be viewed as exhaustive. Ransomware attacks are not always publicly reported by state and local governments and there is no centralized reporting authority, similar to [HIPAA](#) requirements, for these agencies. This means that the number of incidents is most likely underreported. Some ransomware incidents may also be simply reported as a malware attack rather than specifically as a ransomware attack. These incidents would not have been cataloged in the search.

Before diving into the results, I do want to say that most of the incidents would not be widely known if not for the work of local journalists. A lot of the information I was able to find was in local papers or local television news reports, which makes sense — most of these incidents are not “big enough” to be considered national news, so local journalists would be the only ones covering them. Covering cybersecurity is not an easy task, never mind when your typical coverage tends to center on daily business news. We commend these journalists for taking on the effort and are grateful for the work they’re doing.

First, it does appear that ransomware attacks on state and local governments are on the rise. In 2016, I was able to find 46 ransomware attacks. In 2017, that number dropped to 38, which is reflective of a drop in ransomware attacks across all sectors. In 2018, that number jumped to 53, and in the first four months of 2019, there have already been 21 reported attacks. The numbers for 2018 and 2019 may go up, as not all ransomware attacks against state and local governments are reported immediately. Many of the attacks in the catalog were reported weeks or months after they happened, often during city council or budget meetings.

State and Local Government Ransomware Attacks

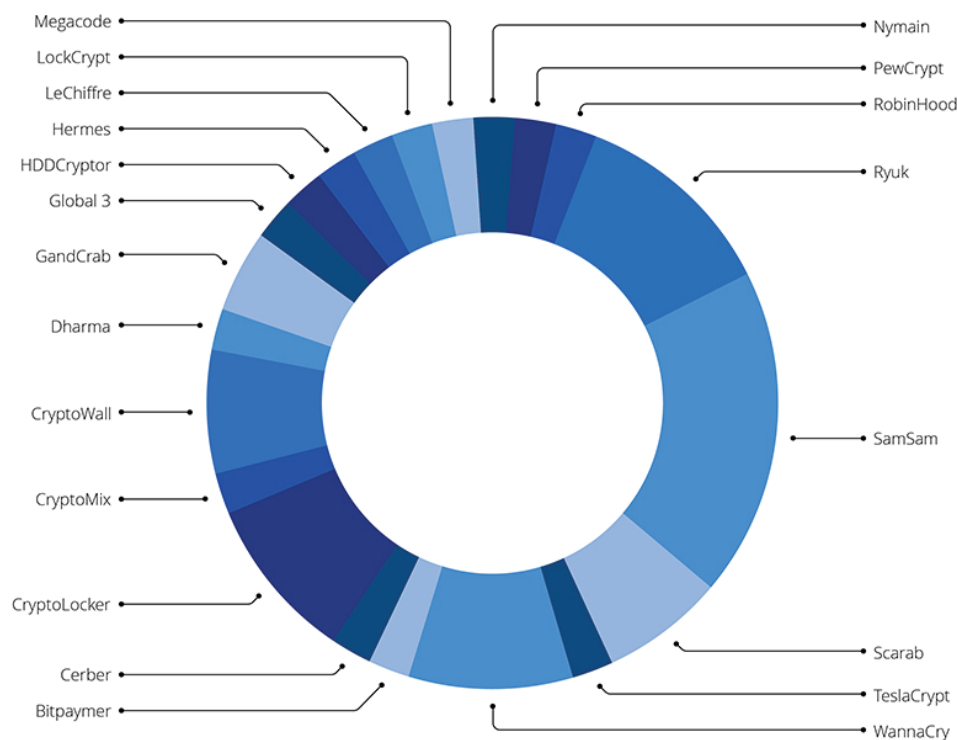


The second finding is that, despite the use of the word “targeted,” it does not appear that these are targeted attacks in the traditional sense. These attacks tend to be more targets of opportunity. Even groups like the teams behind Ryuk and SamSam appear to stumble into these targets. However, once these groups do realize they are in a state or local government target, they take advantage of the fact by targeting the most sensitive or valuable data to encrypt.

A third, and possibly surprising, finding is that state and local governments are less likely than other sectors to pay the ransom. According to a 2019 report from [CyberEdge](#), 45 percent of organizations that were hit with ransomware paid the ransom (this number is up from 38.7 percent in 2018). Based on our analysis, only 17.1 percent of state and local government entities that were hit definitely paid the ransom, and 70.4 percent of agencies confirmed that they did not pay the ransom. Due to limited data availability, I was not able to determine things like which ransomware variants are most often used in these attacks or get a good grasp on the total amounts of ransom demanded.

That being said, I was able to find ransomware attacks that hit 48 states and the District of Columbia. The states with no publicly reported ransomware attacks are Delaware and Kentucky. Note that this does not mean no ransomware attacks occurred, just that they were not publicly reported. For example, this write-up of a [recent attack against Garfield County](#) in Utah mentions that "... the FBI is aware of other ransomware attacks on other Utah governments," but I was unable to find other publicly reported attacks against Utah government agencies. This may be an indication that state and local government ransomware attacks are underreported.

24 of the 169 attacks were against local school systems or colleges. Again, these attacks do not appear to be targeted — it was more a matter of opportunity. 41 of the attacks were against law enforcement offices, though there is some overlap because several attacks that started with local government computers would spread to law enforcement systems as well.



A breakdown of the known types of ransomware used in the attacks. This does not include the category of unidentified pieces of malware, which comprise 76 percent of the total.

Reporting on the type of variant used in these attacks is limited. Only 40 of the 169 reported incidents identified the type of ransomware used in the attack. The variants used in these attacks do seem to mirror the ransomware families used against other sectors. From 2013 to 2016, the primary families reported were CryptoLocker and CryptoWall. In 2017 and 2018, that transitioned to WannaCry and SamSam (though the WannaCry attacks were, unsurprisingly, mostly closely clustered together in May and June of 2017). More recently, in late 2018 and early 2019, the primary ransomware families have been GandCrab and Ryuk.

Overall, ransomware attacks on state and local government agencies are a growing problem. The trend for state and local governments follows an interesting pattern. There was a surge of attacks in 2016, but the number of attacks decreased in 2017. This mirrors ransomware attacks overall for 2016 and 2017. What is interesting is that while 2018 saw a small resurgence in overall ransomware attacks, there was a sharp jump in ransomware attacks against state and local governments, and that surge seems to be continuing into 2019.

Although state and local governments do not pay ransoms nearly as frequently as other targets, they generate outsized media coverage because of the effect these attacks have on the functioning of essential infrastructure and processes. This likely creates a perception among attackers that these are potentially profitable targets. The data shows that the reality is more of a mixed bag — although government agencies are less likely to pay the ransom than other victims, there is still an almost one in five chance that an attacker will get paid. Further, these targets may raise the profile of the attacker (for better or worse) since these agencies are more likely to call in law enforcement and the FBI to assist with the ensuing investigations.

About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.

Date	City	State	Ransomware Family	Ransom Demand	Attribution	Paid	Link	Date	City	State	Ransomware Family	Ransom Demand	Attribution	Paid	Link
Nov, 2013	Swansea PD	MA	CryptoLocker	\$750	—	Y	Source	Oct, 2017	Texas Dept of Agriculture	TX	Unknown	Unknown	—	U	Source
Dec, 2013	Greenland	NH	CryptoLocker	\$300	—	N	Source	Oct, 2017	Yarrow Point	WA	Unknown	\$9,170	—	Y	Source
Jun, 2014	Durham PD	NH	CryptoWall	Unknown	—	N	Source	Nov, 2017	Sacramento Transit System	CA	Unknown	\$8,000	—	N	Source
Jun, 2014	Collinsville PD	AL	Unknown	Unknown	—	N	Source	Nov, 2017	Spring Hill (and 911 Services)	TN	Unknown	\$250,000	—	N	Source
Nov, 2014	Dickson Sheriff Dept	TN	CryptoWall	\$572	—	Y	Source	Dec, 2017	Mecklenburg County (and PD)	NC	LockCrypt	\$23,000	—	N	Source
Feb, 2015	Midlothian PD	IL	Unknown	\$500	—	Y	Source	Dec, 2017	Dept of Agriculture	GA	Unknown	Unknown	—	N	Source
Apr, 2015	Tewksbury	MA	CryptoLocker	\$500	—	Y	Source	Dec, 2017	Jerome School District	ID	Unknown	\$65,000	—	N	Source
Apr, 2015	Lincoln County Police	ME	Megacode	\$300	—	Y	Source	Dec, 2017	Mad River Fire & EMS	OH	Unknown	\$11,400	—	N	Source
Jan, 2016	Medfield	MA	Unknown	\$300	—	Y	Source	Dec, 2017	Nashotah	WI	Unknown	\$2,000	—	Y	Source
Feb, 2016	Park County	WY	TeslaCrypt	Unknown	—	N	Source	Jan, 2018	Farmington	NM	SamSam	\$35,000	—	N	Source
Feb, 2016	Arizona Superior Ct	AZ	Unknown	Unknown	—	N	Source	Jan, 2018	Spartanburg County Library	SC	Unknown	\$35,000	—	N	Source
Feb, 2016	Los Angeles County Health Dept	CA	Unknown	Unknown	—	N	Source	Jan, 2018	Chester County School District	SC	Unknown	Unknown	—	N	Source
Feb, 2016	Oxford School District	MS	Unknown	Unknown	—	N	Source	Jan, 2018	Belle Fourche	SD	Unknown	Unknown	—	N	Source
Feb, 2016	Durham	NC	Unknown	Unknown	—	N	Source	Jan, 2018	Maury County Public Schools	TN	Unknown	Unknown	—	N	Source
Feb, 2016	Horry County School District	SC	Unknown	\$8,000	—	N	Source	Feb, 2018	Colorado Dept of Transportation	CO	SamSam	Unknown	Iran	N	Source
Feb, 2016	Melrose PD	MA	Unknown	\$489	—	Y	Source	Feb, 2018	Davidson County	NC	SamSam	\$23,000	Iran	N	Source
Mar, 2016	Kankakee County	IL	CryptoWall	Unknown	—	N	Source	Feb, 2018	Johnson County Sheriff's Dept	AR	Unknown	None	—	N	Source
Mar, 2016	Manlius	NY	LeChiffre	\$400	Russia	N	Source	Feb, 2018	Hinesville	GA	Unknown	Unknown	—	N	Source
Mar, 2016	Cloquet School District	MN	Unknown	\$6,000	—	N	Source	Feb, 2018	Connecticut State Agencies	CT	WannaCry	\$48,000	North Korea	N	Source
Mar, 2016	Clark County Water Reclamation	NV	Unknown	Unknown	—	U	Source	Feb, 2018	Savannah (and Savannah PD)	GA	Unknown	Unknown	—	Y	Source
Apr, 2016	Plainfield	NJ	Unknown	\$650	—	N	Source	Mar, 2018	Plymouth & Plymouth PD	CT	GandCrab	Unknown	—	N	Source
Apr, 2016	Lansing Board of Water and Light	MI	Unknown	\$25,000	—	Y	Source	Mar, 2018	Colorado Dept of Transportation	CO	SamSam	Unknown	Iran	N	Source
May, 2016	Pinal County Attorney's Office	AZ	CryptoLocker	Unknown	—	N	Source	Mar, 2018	Atlanta (and Atlanta PD)	GA	SamSam	\$55,000	Iran	N	Source
May, 2016	Grant County Education Service District	OR	Scarab	Unknown	—	N	Source	Mar, 2018	Portland	CT	Unknown	\$2,000	—	N	Source
May, 2016	Rhinebeck School District	NY	Unknown	\$500	—	N	Source	Mar, 2018	Portland (II)	CT	Unknown	\$2,000	—	N	Source
Jun, 2016	Henry County 911	TN	Scarab	Unknown	—	N	Source	Mar, 2018	Connecticut Judicial Branch	CT	Unknown	Unknown	—	N	Source
Jun, 2016	Palm Beach 911 Services	FL	Unknown	Unknown	—	N	Source	Mar, 2018	Baltimore 911 System	MD	Unknown	Unknown	—	N	Source
Jun, 2016	Janesville	WI	Unknown	Unknown	—	U	Source	Mar, 2018	Mississippi Valley State University	MS	SamSam	Unknown	Iran	U	Source
Jun, 2016	Columbiana County Juvenile Court	OH	Unknown	\$2,883	—	Y	Source	Mar, 2018	Leeds (City, FD and PD)	AL	Unknown	\$8,000	—	Y	Source
Jul, 2016	Woodbury County	IA	Unknown	Unknown	—	N	Source	Apr, 2018	Dawson County	GA	Unknown	Unknown	—	N	Source
Jul, 2016	Wadena	MN	Unknown	Unknown	—	N	Source	Apr, 2018	Ashland Community Library	ME	Unknown	\$400	—	N	Source
Aug, 2016	Sarasota	FL	Unknown	\$33,000,000	—	N	Source	Apr, 2018	Rockport	ME	Unknown	\$1,000	—	N	Source
Aug, 2016	State Police	RI	Unknown	Unknown	—	N	Source	Apr, 2018	Riverside FD & PD	OH	Unknown	Unknown	—	N	Source
Aug, 2016	Barnstable PD	MA	Unknown	Unknown	—	N	Source	Apr, 2018	Richmond	VA	Unknown	Unknown	—	N	Source
Sep, 2016	Yuba City	CA	Unknown	Unknown	—	N	Source	Apr, 2018	Leominster School District	MA	Unknown	\$10,000	—	Y	Source
Sep, 2016	Palm Beach 911 Services	FL	Unknown	Unkonwn	—	N	Source	May, 2018	Pasquotank	NC	Scarab	\$2,500	—	N	Source
Sep, 2016	Honolulu, FD	HI	Unknown	Unknown	—	N	Source	May, 2018	Winder	GA	Unknown	\$320,000	—	N	Source
Sep, 2016	Crow Wing County	MN	Unknown	Unknown	—	N	Source	May, 2018	Riverside FD & PD	OH	Unknown	Unknown	—	N	Source
Sep, 2016	Dep of Mineral Resources	ND	Unknown	\$350	—	N	Source	May, 2018	Roseburg Public Schools	OR	Unknown	Unknown	—	N	Source
Sep, 2016	Springfield	TN	Unknown	\$1,000	—	N	Source	Jun, 2018	Jefferson Village	OH	Unknown	\$4,900	—	N	Source
Sep, 2016	Palm Hill PD	TX	Unknown	\$250	—	U	Source	Jun, 2018	State Agencies	RI	Unknown	Unknown	—	N	Source
Oct, 2016	Henry County	OH	Unknown	Unknown	—	N	Source	Jun, 2018	Middletown School District	CT	Unknown	Unknown	—	U	Source
Oct, 2016	Mount Holly Springs PD	PA	Unknown	\$500	—	N	Source	Jul, 2018	Mat-Su	AK	Bitpayer	\$400,000	—	N	Source
Nov, 2016	San Francisco Muni	CA	HDDCryptor	\$73,000	—	N	Source	Jul, 2018	Derby Police Dept	CT	Unknown	Unknown	—	N	Source
Nov, 2016	Howard County	IN	Unknown	Unknown	—	N	Source	Jul, 2018	Valdez	AK	Hermes	\$26,000	—	Y	Source
Nov, 2016	St Mary's County	MD	Unknown	Unknown	—	N	Source	Jul, 2018	Westmoreland County Housing Authority	PA	Unknown	\$6,500	—	Y	Source
Nov, 2016	Bigfork School District	MT	Unknown	Unknown	—	N	Source	Aug, 2018	Coweta County and Public Safety	GA	Unknown	Unknown	—	N	Source
Nov, 2016	Madison County (and PD)	IN	Unknown	\$21,000	—	Y	Source	Aug, 2018	Cloquet School District	MN	Unknown	Unknown	—	N	Source
Dec, 2016	Alpena School System	MI	Unknown	Unknown	—	N	Source	Sep, 2018	Monroe County School District	FL	GandCrab	Unknown	—	N	Source
Dec, 2016	Mt Pleasant PD	SC	Unknown	Unknown	—	N	Source	Sep, 2018	Port of San Diego (Harbor and PD)	CA	SamSam	Unknown	Iran	N	Source
Dec, 2016	Cockrell Hill Police Dept	TX	Unknown	\$4,000	—	N	Source	Sep, 2018	Marblehead	MA	Unknown	Unknown	—	N	Source
Dec, 2016	Allegheny County State Prosecutor	PA	Nymain	\$1,400	—	Y	Source	Sep, 2018	Beatrice (and PD & FD)	NE	Unknown	Unknown	—	U	Source
Dec, 2016	Carroll County Sheriff's Dept	AR	Unknown	\$2,400	—	Y	Source	Oct, 2018	Onslow County Water and Sewer	NC	Ryuk	Unknown	—	N	Source
Dec, 2016	Los Angeles Valley College	CA	Unknown	\$28,000	—	Y	Source	Oct, 2018	Muscatine (City & PD)	IA	Unknown	Unknown	—	N	Source
Dec, 2016	Bighton PD	MA	Unknown	\$4,600	—	Y	Source	Oct, 2018	Madison County	ID	Unknown	Unknown	—	N	Source
Jan, 2017	Washington	DC	Cerber	Unknown	—	N	Source	Oct, 2018	Moultrie County	IL	Unknown	Unknown	—	U	Source
Jan, 2017	Marion County	FL	Unknown	Unknown	—	N	Source	Oct, 2018	Crawford County	IL	Unknown	Unknown	—	U	Source
Jan, 2017	St Louis Public Library	MO	Unknown	\$35,000	—	N	Source	Oct, 2018	Indiana National Guard	IN	Unknown	Unknown	—	U	Source
Jan, 2017	Kanawha County Board of Education	WV	Unknown	Unknown	—	N	Source	Oct, 2018	West Haven	CT	Unknown	\$2,000	—	Y	Source
Jan, 2017	Warren County Sheriff's Dept	MO	CryptoMix	Unknown	—	U	Source	Nov, 2018	Rockaway Township PD	NJ	Unknown	Unknown	—	U	Source
Feb, 2017	Bingham County (and Dispatch	ID	Unknown	\$30,000	—	N	Source	Nov, 2018	Johannesburg-Lewiston School Distric	MI	Unknown	Unknown	—	Y	Source
Feb, 2017	Roxana Police Department	IL	Unknown	Unknown	—	N	Source	Dec, 2018	North Bend (and PD)	OR	PewCrypt	\$50,000	Romania	N	Source
Feb, 2017	Office of Management and Enterprise	OK	Unknown	Unknown	—	N	Source	Dec, 2018	Jupiter	FL	Unknown	Unknown	—	N	Source
Feb, 2017	Licking County	OH	Unknown	Unknown	—	Y	Source	Jan, 2019	Lamar County Sheriff's Dept	TX	Dharma	Unknown	—	N	Source
Mar, 2017	PA State Senate Democrats	PA	Unknown	Unknown	—	N	Source	Jan, 2019	Salisbury PD	MD	Unknown	Unknown	—	N	Source
Mar, 2017	Wood River Police Department	IL	Unknown	Unknown	—	N	Source	Jan, 2019	Akron	OH	Unknown	Unknown	—	N	Source
Apr, 2017	Troup County (and PD)	GA	Unknown	\$39,600	Eastern Europe	N	Source	Jan, 2019	Sammamish	WA	Unknown	Unknown	—	N	Source
Apr, 2017	Perkin High School	IL	Unknown	\$37,000	—	N	Source	Jan, 2019	Bridgeport School Systems	CT	Unknown	Unknown	—	U	Source
Apr, 2017	Forsyth Public Schools	MT	Unknown	Unknown	—	N	Source	Jan, 2019	Del Rio	TX	Unknown	Unknown	—	U	Source
Apr, 2017	Newark	NJ	SamSam	\$30,000	Iran	Y	Source	Feb, 2019	Colchester	CT	Unknown	Unknown	—	N	Source
May, 2017	Cook County	IL	WannaCry	Unknown	North Korea	N	Source	Feb, 2019	Mt Zion School District	IL	Unknown	Unknown	—	N	Source
May, 2017	Murfreesboro PD & FD	TN	WannaCry	Unknown	North Korea	N	Source	Feb, 2019	Taos Municipal School District	NM	Unknown	\$5,000	—	N	Source
Jun, 2017	Rensselaer County Library	NY	WannaCry	Unknown	North Korea	N	Source	Mar, 2019	Committee for Public Counsel	MA	Ryuk	Unknown	—	N	Source
Jul, 2017	Marion County Fairgrounds	IN	Unknown	\$1,000	—	N	Source	Mar, 2019	Park Rapids School System	MN	Unknown	Unknown	—	N	Source
Jul, 2017	Cape May County	NJ	Unknown	Unknown	—	U	Source	Mar, 2019	Orange County (and PD)	NC	Unknown	Unknown	—	N	Source
Jul, 2017	Brownsburg Public Library	IN	Unknown	\$1,000	—	Y	Source	Mar, 2019	Fisher County PD	TX	Unknown	Unknown	—	N	Source
Aug, 2017	Iberia Parish Sheriff's Office	LA	Unknown	Unknown	—	N	Source	Mar, 2019	Albany	NY	Unknown	Unknown	—	U	Source
Aug, 2017	Washington	MO	Unknown	Unknown	—	N	Source	Mar, 2019	Jackson County	GA	Ryuk	\$400,000	—	Y	Source
Aug, 2017	Becker County	MN	Unknown	Unknown	—	U	Source	Apr, 2019	Genessee County	MI	Unknown	Unknown	—	N	Source
Aug, 2017	Dorchester School District	SC	Unknown	\$2,900	—	Y	Source	Apr, 2019	Imperial County	CA	Ryuk	Unknown	—	N	Source
Sep, 2017	St Johnsbury	VT	Global 3	\$250	—	N	Source	Apr, 2019	Stuart	FL	Ryuk	Unknown	—	N	Source
Sep, 2017	Butler County (and PD)	KS	Unknown	Unknown	—	U	Source	Apr, 2019	Greenville	NC	RobinHood	Unknown	—	U	Source
Sep, 2017	Indianhead Library System	WI	Unknown	Unknown	—	U	Source	Apr, 2019	Augusta	ME	Unknown	Unknown	—	U	Source
Oct, 2017	Englewood	CO	Unknown	Unknown	—	N	Source	Apr, 2019	Garfield County	UT	Unknown	Unknown	—	Y	Source
Oct, 2017	Topsham	ME	Unknown	Unknown	—	N	Source								