Ransomware Hits Georgia Courts as Municipal Attacks Spread

Ransomware has no shortage of cautionary tales[1] and wakeup calls[2] from the past decade. But for local governments, this past year has been a particularly brutal reminder of the threat. Following a 2018 attack that paralyzed the City of Atlanta[3] for weeks, more than half a dozen cities and public services across the country have fallen to ransomware so far in 2019, on a near-monthly basis; the Administrative Office of the Georgia Courts became the latest victim on Saturday, when an attack knocked[4] its systems offline.

The string of attacks on municipalities may seem like a new pattern. But it's unclear how many of them, if any, were perpetrated by the same actors. And law enforcement officials emphasize that the spate of attacks actually fits into a broader, ever-growing trend of ransomware attacks that spans numerous industry sectors.

"We are seeing an increase in targeted ransomware attacks; however, we do not have enough data to indicate one industry or sector is being targeted more than another," the FBI told WIRED in a statement. "Cyber criminals are opportunistic. They will monetize any network to the fullest extent."

Incident responders agree with this assessment and note that attackers will capitalize on any technique that sees some success, to infect as many targets as possible and maximize the possibility of return.

"There's definitely an increase or uptick in the amount of ransomware campaigns that we're seeing out there, but it's not specific to municipalities or state or federal organizations, it's just pretty much across the board in every industry vertical," says David Kennedy, CEO of the penetration testing and incident response consultancy TrustedSec. "We're working seven consecutive ransomware attacks right now—a couple of manufacturing, a couple of credit unions, and one local type of government incident."

One thing that does set cities and municipalities apart is that they are more likely to publicly disclose attacks and the ransom amounts criminals are seeking, because the attacks often disrupt public systems. Where organizations like businesses and hospitals sometimes have more leeway to work behind closed doors, attacks on government entities can be more immediately visible. And whether a local government is going to rebuild from an attack on its own or pay the ransom, money to respond comes from public funds or through a municipality's cybersecurity insurance. And lately, some municipalities have been very vocally coughing up the cash to hackers.

In March, ransomware hit[5] the court system in rural Jackson County Georgia, between Atlanta and Athens. Jackson County paid attackers[6] $400,000. And throughout June, three Florida municipalities[7]—Key Biscayne, Lake City, and Riviera Beach—were hit with ransomware. Lake City paid 42 bitcoin (almost $500,000) to attackers, and Riviera Beach paid 65 bitcoin (almost $600,000).

"While the size of recent payouts are certainly not groundbreaking, publicly reporting on them is," says Jake Williams, founder of the Georgia-based security firm Rendition Infosec. "There are tons of targets out there, and most of them don't realize they have the exposure. I've never worked a ransomware case where a victim said 'we realized this could happen to us but were playing the odds it wouldn't.' Most of them have heard of ransomware but fail to realize they have an exposure."

Desperate organizations have long paid ransoms as a sort of last-ditch, dirty secret when they don't think they can recover any other way. But incident responders suggest that the recent disclosures may only further fuel attackers' enthusiasm to hit as many local-level government targets as possible. In April, ransomware struck email and baggage systems[8] at Cleveland Hopkins International Airport. In May, Baltimore City was crippled by ransomware, as was the Philadelphia Courts[9] First Judicial District.

On Monday, the Administrative Office of the Georgia Courts (a coordinating agency, not the courts themselves) had its website go down as it scrambled to contain the infection. Spokesperson Bruce Shaw told WIRED that the agency could not yet comment on the type of ransomware used in the attack but had seen no evidence of data exfiltration. He added that the systems being held for ransom do not contain personally identifying information. "On Saturday morning the Administrative Office of the Courts discovered sophisticated malware on our servers. After an assessment of our system, it was determined that it would be best to take our network offline," the agency said in a prepared statement provided by Shaw. "Our primary focus at this time is to ensure our systems remain secure and that we get them back up and running as soon as possible."

The actors behind these recent incidents are largely unknown. Two of the three attacks in Florida involved the well-known ransomware called Ryuk, and some preliminary reports have indicated that this ransomware[10] may currently be at work in the Georgia incident as well. But while this malware was first spotted in 2018 being used by hackers linked to North Korea, it seems to be in broad criminal circulation now and is therefore more difficult to attribute to a particular attacker. In general, ransomware attacks are a sort of pay-to-play market, in which technically sophisticated criminal syndicates offer malware and attack services to virtually anyone on the black market.

Conventional wisdom, as well as the official recommendation[11] of the US government, is to never pay hackers' ransoms. If they're not getting paid, they won't have an incentive to keep trying.

"The payment of extortion demands encourages continued criminal activity, leads to other victimizations, and can be used to facilitate additional serious crimes," the FBI told WIRED in its statement. "Additionally, paying a ransom does not guarantee the victim will regain access to their data … The main thrust of the FBI's ransomware outreach program is to inform the public that most ransomware can be prevented."

Though ransomware has been a ubiquitous threat for years, investment hasn't come fast enough to address the risk, especially in settings like local government, where IT departments are chronically understaffed and underfunded. And incident responders note that for those who are unprepared, the reality of the decision about whether to pay is often fraught.

"My recommendation is do not pay the ransom under any circumstance," Kennedy says. "But it's not always a clear-cut issue. We had one case where we had a church that lost 20 years of their sermons in a ransomware attack, and that was a big deal for them. If an organization can pay $10,000 or $20,000 to recover, sometimes they're going to lean more toward paying."

As a result, ransomware scams are still extremely lucrative for attackers. One group, GandCrab, that offered a popular "ransomware as a service" platform shut down at the beginning of June[12]. But it wasn't because of a law enforcement sting or an uptick in impenetrable defense—the hackers behind the service claim it was because they had just made *so much money* that they didn't need to go on. "We are leaving for a well-deserved retirement," the actors wrote in a forum post. "We have proved that by doing evil deeds, retribution does not come." They claim to have collected more than $2 billion in ransom payments, with those running the service getting about $2.5 million per week.

These attacks can come at a high cost to local governments, whether they pay attackers or not. It cost Atlanta about $17 million[13] to recover from its 2018 attack. Baltimore City has spent about $18 million[14] to recover and improve its defenses.

For organizations that don't have the will or resources to invest in ransomware defenses now, every day is a gamble that they won't pay for it later.

More Great WIRED Stories

- He cyberstalked girls for years—then they fought back[15]
- One boy's dream vacation to see construction equipment[16]
- Notifications are stressing us out. How did we get here[17]?
- How nine people built an illegal $5 million Airbnb empire[18]
- Everything you want—and need—to know about aliens[19]
- 🏹🔳♀ Want the best tools to get healthy? Check out our Gear team's picks for the best fitness trackers[20], running gear[21] (including shoes[22] and socks[23]), and best headphones[24].
- 📩 Get even more of our inside scoops with our weekly Backchannel newsletter[25]

Links

1. https://www.wired.com/2017/05/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/
2. https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/
3. https://www.wired.com/story/atlanta-ransomware-samsam-will-strike-again/
4. https://www.11alive.com/article/news/local/georgia-court-system-hit-by-malware-attack/85-1c8d8672-b7ed-4c12-a5f4-f4be6a626834
5. https://www.11alive.com/article/tech/ransomware-attack-targets-rural-georgia-county/85-2d6459e7-bd16-4cf9-b9fb-b03108a25144
6. https://www.zdnet.com/article/georgia-county-pays-a-whopping-400000-to-get-rid-of-a-ransomware-infection/
7. https://arstechnica.com/information-technology/2019/06/is-there-something-in-the-water-third-florida-city-hit-by-ransomware/

8. https://www.news5cleveland.com/news/local-news/cleveland-metro/ransomware-infected-cleveland-hopkins-international-airports-computing-systems-fbi-confirms

9. https://billypenn.com/2019/06/26/philly-courts-website-is-finally-back-after-not-russian-virus-attack/

10. https://arstechnica.com/information-technology/2019/07/ryuk-ryuk-ryuk-georgias-courts-hit-by-ransomware/

11. https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

12. https://www.zdnet.com/article/gandcrab-ransomware-operation-says-its-shutting-down/

13. https://statescoop.com/one-year-after-atlantas-ransomware-attack-the-city-says-its-transforming-its-technology/

14. https://arstechnica.com/information-technology/2019/06/baltimores-bill-for-ransomware-over-18-million-so-far/

15. https://www.wired.com/story/cyberstalked-teen-girls-for-years-fought-back/?itm_campaign=BottomRelatedStories_Sections_1

16. https://www.wired.com/story/one-boys-dream-vacation-to-see-giant-construction-equipment/?itm_campaign=BottomRelatedStories_Sections_1

17. https://www.wired.com/story/history-of-notifications/?itm_campaign=BottomRelatedStories_Sections_1

18. https://www.wired.com/story/how-9-people-built-illegal-5m-airbnb-empire-new-york/?itm_campaign=BottomRelatedStories_Sections_1

19. https://www.wired.com/story/wired-guide-aliens/?itm_campaign=BottomRelatedStories_Sections_1

20. https://www.wired.com/gallery/best-fitness-tracker/?itm_campaign=BottomRelatedStories

21. https://www.wired.com/gallery/best-running-gear/?itm_campaign=BottomRelatedStories

22. https://wired.com/gallery/best-trail-running-shoes-round-up/?itm_campaign=BottomRelatedStories

23. https://www.wired.com/gallery/best-running-socks/?itm_campaign=BottomRelatedStories

24. https://www.wired.com/gallery/best-headphones-under-100/?itm_campaign=BottomRelatedStories

25. https://www.wired.com/newsletter/?name=backchannel&sourceCode=BottomStories