TechRepublic.

Small municipalities suffer the majority of ransomware, but they aren't the only ones suffering as ransoms rise and payouts become more common.

Image: vchal, iStockphoto

Barracuda Networks' analysis of ransomware attacks over the past 12 months found that local municipal governments continue to be the preferred target, the amount of ransom demanded is on the rise, and more people are paying out. Combined, those three facts mean ransomware isn't going away anytime soon. In fact, Barracuda found it's increasingly being used in conjunction with data breaches as well, with 41% of attacks combining the two.

The reasons for this two-fronted attack are obvious: Not only can an attacker make additional money selling stolen data, they can also leverage private or sensitive information as part of the ransom demand.

Municipal governments were subject to 45% of ransomware attacks in the past 12 months, and the other two sectors leading were healthcare with 22%, and education with 15%. Corporations, which made up 27% of ransomware targets in the previous year, dropped to just 14% of targets. Logistics companies, which previously weren't a target at all, have started to be noticed as well, accounting for 5% of ransomware attacks in the past 12 months.

Barracuda said that healthcare ransomware attacks are unsurprising, with a multitude of cybersecurity threats against medical institutions being reported during the COVID-19 pandemic. Education, Barracuda said, is a hotbed of valuable sensitive data, and logistics companies are increasingly important for their ability to distribute much-needed protective equipment and goods being bought online due to coronavirus lockdowns.

The report also cites an increase in the demands of ransomware attackers, with the average payment in the past 12 months being $1,652,666. This can be especially devastating to municipal targets: All of those who were attacked and paid out were in areas with less than 50,000 people who simply didn't have the resources to manually recover from an attack.

Fifteen percent of municipalities who have been attacked in the past 12 months paid the demanded ransom; Barracuda noted that "practically none" of targeted municipalities paid ransoms over the previous 12 months.

Countering the persistent threat of ransomware

Payouts are more frequent, and ransoms are rising: Those facts alone should be enough to conclude that ransomware is going to continue being a threat. The only way to counter this rise is to make it more of a hassle for attackers to launch a successful attack, and Barracuda offered several recommendations for making that possible.

- **Use a spam filter and phishing detection system:** With so many malicious emails appearing to be legitimate, artificial intelligence (AI)-powered filters can pick up on subtle clues that a reader may miss.
- **Advanced firewalls can stop malware from reaching out:** Malicious attachments are a common way to trick users into malware, and those attachments typically have to reach out to a command-and-control server

to download their payloads. Firewalls capable of malware analysis can stop these connections from happening.

- **Malware detection is essential:** Good antimalware software can detect when a document is trying to download an executable file, which Barracuda said no document should ever do.
- **Use, and actively maintain, blacklists:** Attackers frequently reuse IP addresses to host malware and run botnets. A blacklist that's regularly updated with known bad IP addresses can stop an attack from ever starting.
- **Train your users:** Phishing simulations, bulletins, and training can go a long way to transform the weakest security link into an asset.
- **Good backups are essential:** A ransomware attack can be easily negated if you're able to simply roll back your systems to a previous good state. Barracuda recommends the 3-2-1 backup rule: Make three copies of essential files on two different media types, and maintain at least one backup offsite.