Threat Spotlight: Government Ransomware Attacks

blog.barracuda.com/2019/08/28/threat-spotlight-government-ransomware-attacks/

Fleming Shi

August 28, 2019

Cybercriminals are targeting state and local governments across the United States with ransomware.

Barracuda researchers have identified more than 50 cities and towns attacked so far this year. The team's recent analysis of hundreds of attacks across a broad set of targets revealed that government organizations are the intended victims of nearly two-thirds of all ransomware attacks. Local, county, and state governments have all been targets, including schools, libraries, courts, and other entities.

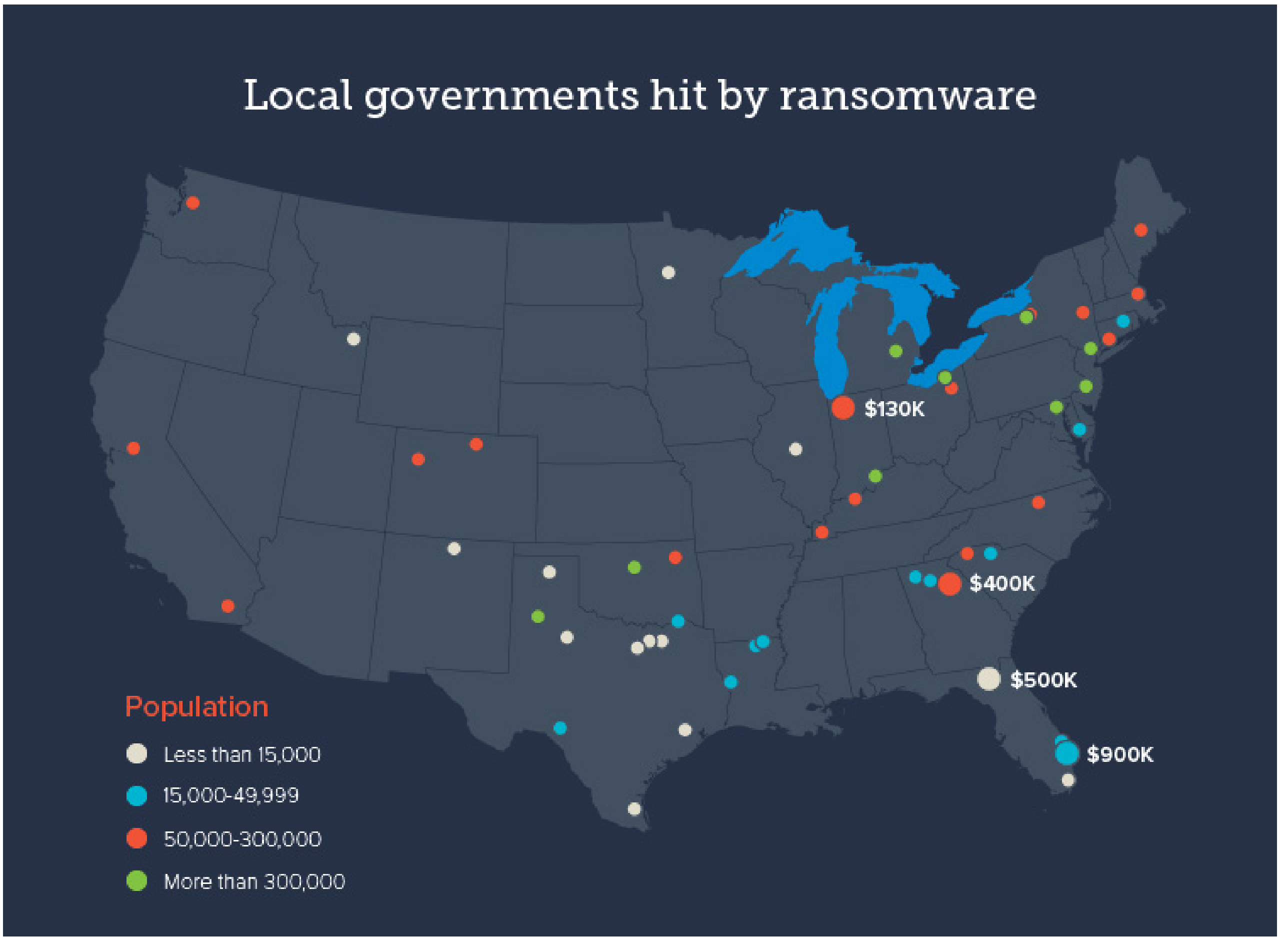
Here's a closer look at state and local government ransomware attacks and solutions to help detect, block, and recover from them.

Note: When the following analysis was completed, only five of the 22 Texas communities affected by a coordinated ransomware attack had been identified. Because the other towns were not yet named, they could not be included in this analysis. Counting those 17 communities brings the total number of ransomware attacks on state and local government in 2019 to just above 70.

More than 70 state and local governments have been hit with #ransomware so far in 2019 Click To Tweet

Highlighted Threat

Municipal Ransomware Attacks — Cybercriminals use malicious software, delivered as an email attachment or link, to infect the network and lock email, data and other critical files until a ransom is paid. These evolving and sophisticated attacks are damaging and costly. They can cripple day-to-day operations, cause chaos, and result in financial losses from downtime, ransom payments, recovery costs, and other unbudgeted and unanticipated expenses.



The Details

The first reported government ransomware attack took place in 2013 on the small town of Greenland, New Hampshire. While ransomware has been around for about 20 years, the threat has been growing rapidly recently, especially when it comes to attacks on government. According to Cybersecurity Ventures, ransomware damages are predicted to rise to $11.5 billion in 2019, up $3.5 billion from last year. Municipalities are among the three biggest targets.

Barracuda researchers analyzed 55 ransomware attacks on state, county, and local governments that have taken place this year. Of the 55 attacks, 38 were on local governments, 14 were on county governments, and three were on state governments. While all types of governments were affected, most victims were small towns or big cities.

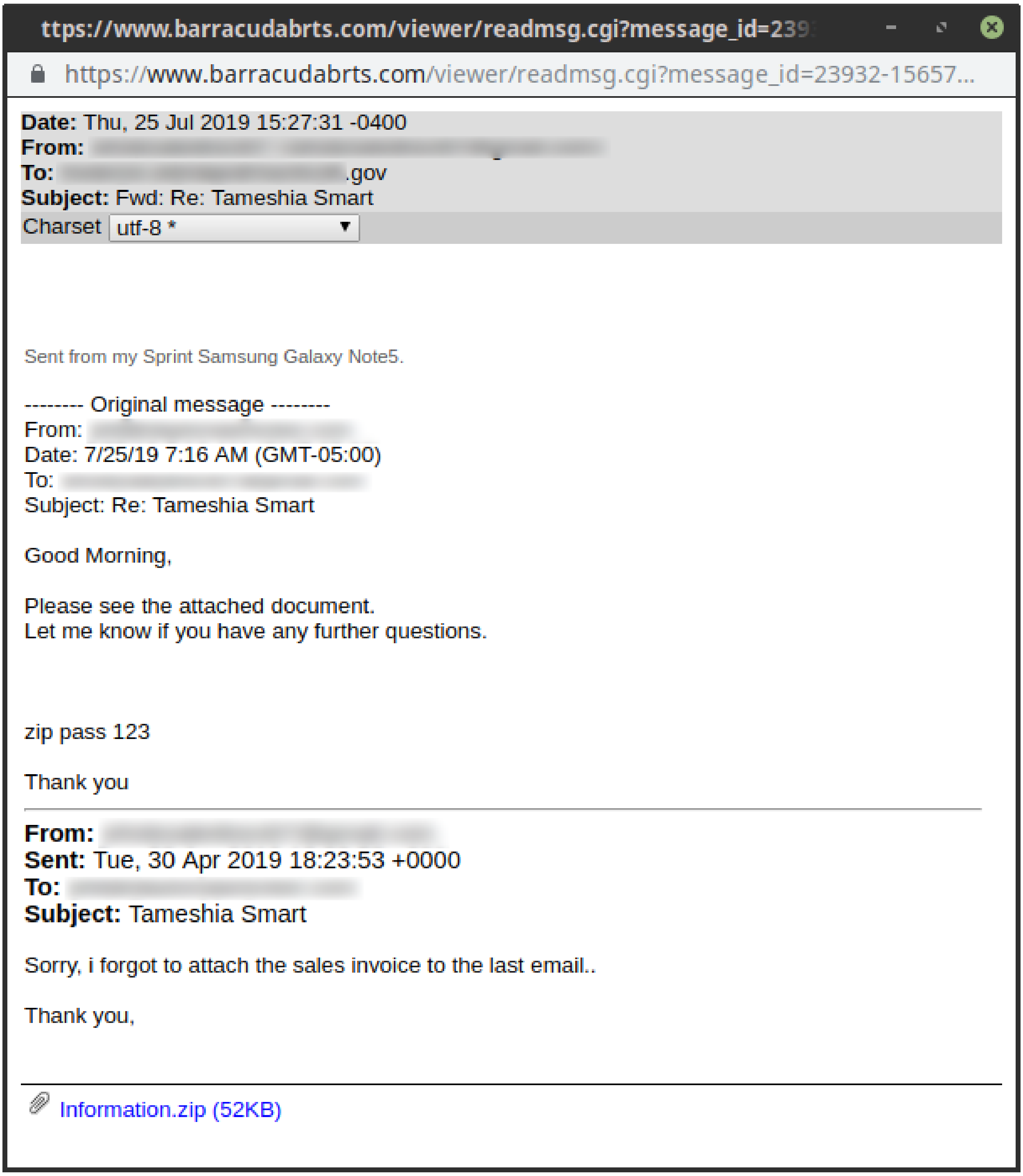
About 45 percent of the municipalities attacked had populations of less than 50,000 residents, and 24 percent had less than 15,000 residents. Smaller towns are often more vulnerable because they lack the technology or resources to protect against ransomware attacks. Nearly 16 percent of the municipalities attacked were cities with populations of more than 300,000 residents.

About 45 percent of the municipalities attacked by #ransomware so far in 2019 had populations of less than 50,000 residents, and 24 percent had less than 15,000 residents.Click To Tweet

In the 55 attacks this year, only two town governments and one country government paid the ransom, all in June. In Florida, Lake City paid roughly $500,000 (42 Bitcoin), and Riviera Beach paid about $600,000 (65 Bitcoin), after trying and failing to recover their data. In Indiana, La Porte County paid $130,000 to recover its data. None of the cities attacked in 2019 so far have paid a ransom, including Baltimore, which spent $18 million to recover from the attack.

Ransomware used in recent attacks against state and local governments includes Ryuk, SamSam, LockerGoga and RobbinHood.

Barracuda researchers see attacks like this against government organizations on a regular basis. Below is a recent example of an email-borne ransomware attack, detected through Barracuda's threat intelligence layers. Email is the most common threat vector for these types of ransomware attacks, but the blast radius can easily reach networks, applications and a wide variety of sensitive and critical data.



ttps://www.barracudabrts.com/viewer/readmsg.cgi?message_id=239

https://www.barracudabrts.com/viewer/readmsg.cgi?message_id=23932-15657...

Date: Thu, 25 Jul 2019 15:27:31 -0400
From: [redacted] [redacted]
To: [redacted].gov
Subject: Fwd: Re: Tameshia Smart
Charset utf-8 *

Sent from my Sprint Samsung Galaxy Note5.

-------- Original message --------
From: [redacted]
Date: 7/25/19 7:16 AM (GMT-05:00)
To: [redacted]
Subject: Re: Tameshia Smart

Good Morning,

Please see the attached document.
Let me know if you have any further questions.

zip pass 123

Thank you

From: [redacted]
Sent: Tue, 30 Apr 2019 18:23:53 +0000
To: [redacted]
Subject: Tameshia Smart

Sorry, i forgot to attach the sales invoice to the last email..

Thank you,

Information.zip (52KB)

While this study focused on attacks in the United States, there have been similar attacks globally, with attacks hitting four communities of varying sizing in Canada as well the Dublin tram system in Ireland and power utilities in India and South Africa.

Government organizations at all levels need preventative and defensive strategies in place, along with disaster and recovery capabilities.

Government organizations at all levels need preventative and defensive strategies in place, along with disaster and recovery capabilities. #ransomwareClick To Tweet

Defending Against Ransomware Attacks

The rapidly evolving email threat environment requires advanced inbound and outbound security techniques that go beyond the traditional gateway, including closing the technical and human gaps, to maximize security and minimize the risk of falling victim to sophisticated ransomware attacks.

Spam Filters / Phishing-Detection Systems
While many malicious emails appear convincing, spam filters, phishing-detection systems and related security software can pick up subtle clues and help block potentially threatening messages and attachments from reaching email inboxes.

Advanced Firewall
If a user opens a malicious attachment or clicks a link to a drive-by download, an advanced network firewall capable of malware analysis provides a chance to stop the attack by flagging the executable as it tries to pass through.

Malware Detection
For emails with malicious documents attached, both static and dynamic analysis can pick up on indicators that the document is trying to download and run an executable, which no document should ever be doing. The URL for the executable can often be flagged using heuristics or threat intelligence systems. Obfuscation detected by static analysis can also indicate whether a document may be suspicious.

Blacklists
With IP space becoming increasingly limited, spammers are increasingly using their own infrastructure. Often, the same IPs are used long enough for software to detect and blacklist them. Even with hacked sites and botnets, once a large enough volume of spam has been detected, it's possible to temporarily block attacks by IP.

User-Awareness Training
Make phishing simulation part of security awareness training to ensure end users can identify and avoid attacks. Transform them from a security liability into a line of defense by testing the effectiveness of in-the-moment training and evaluating the users most vulnerable to attacks.

Backup
In the event of an attack, a cloud backup solution can minimize downtime, prevent data loss, and get your systems restored quickly, whether your files are located on physical devices, in virtual environments, or the public cloud. Ideally, you should follow the 3-2-1 rule of backup with three copies of your files on two different media types with at least one offsite to avoid having backups affected by a ransomware attack.

See what threats are hiding in your Office 365 mailboxes

This Threat Spotlight was authored by Fleming Shi with research support from Audrey Laude of the Barracuda Research team.