Local Governments Held for Ransom

LESSONS LEARNED FROM THE ATLANTA CYBER ATTACK

October 21, 2018

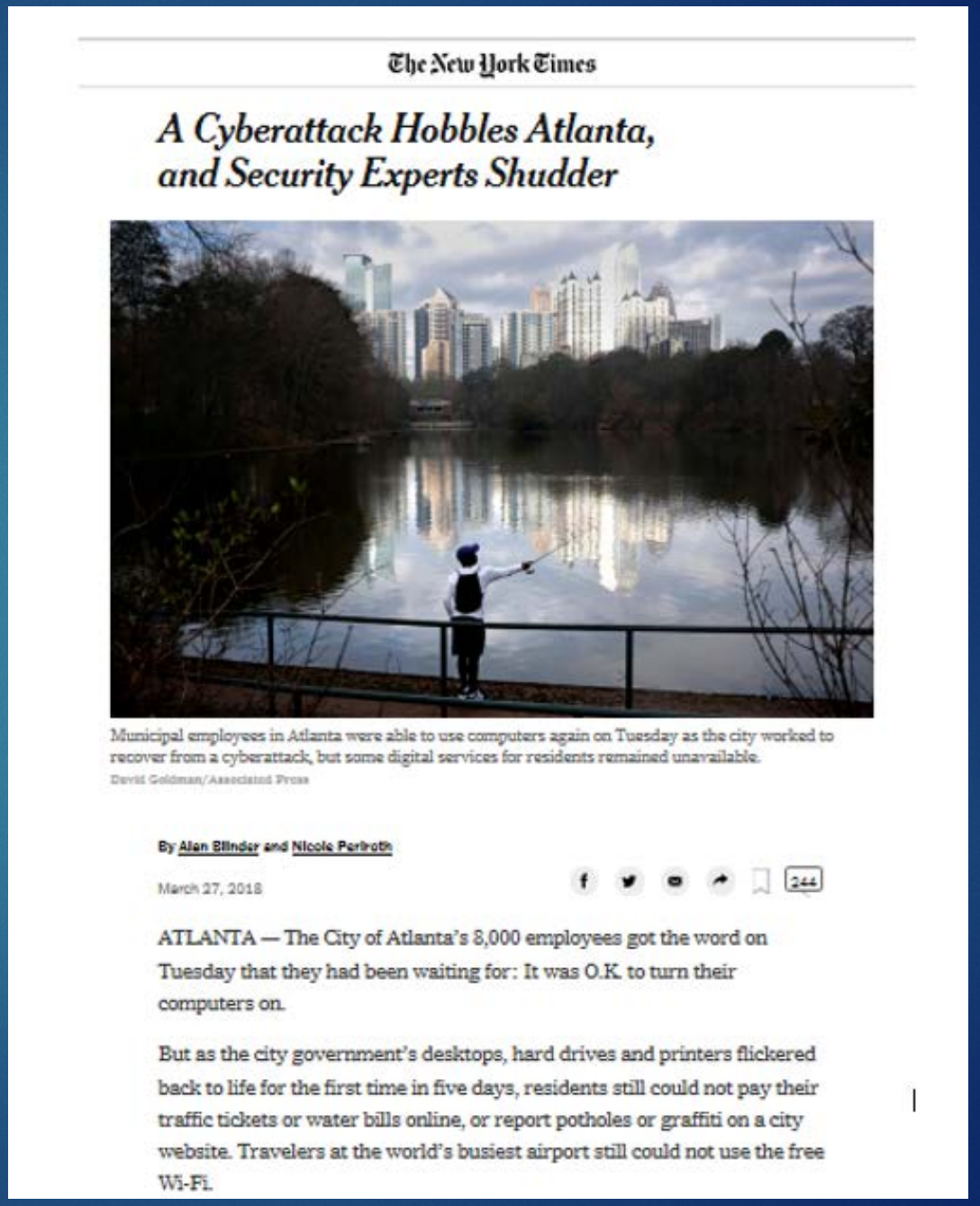
Rhonda Collins - Asst. City Attorney, City of Atlanta
Roy E. Hadley - Special Counsel, Adams and Reese, LLP

Agenda

- Introduction
- Ransomware Attack Basics
- City of Atlanta
- Best Practices
- Questions

Recent Attacks

- Equifax
- Home Depot
- Sony Pictures
- FedEx
- Savannah, GA
- Dallas, TX
- Baltimore, MD



The New York Times

A Cyberattack Hobbles Atlanta, and Security Experts Shudder

Municipal employees in Atlanta were able to use computers again on Tuesday as the city worked to recover from a cyberattack, but some digital services for residents remained unavailable.
David Goldman/Associated Press

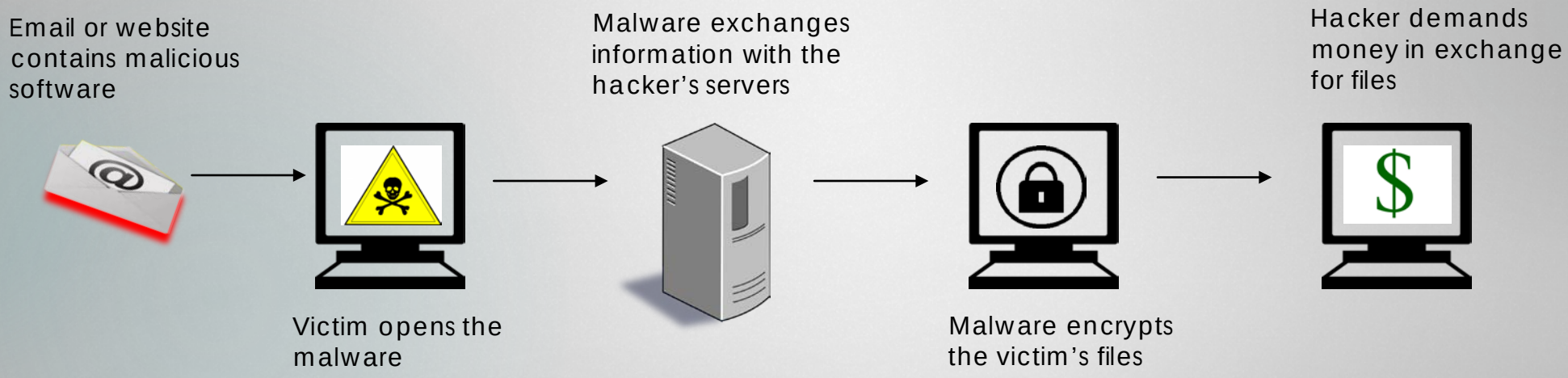
By Alan Blinder and Nicole Perlroth

March 27, 2018

ATLANTA — The City of Atlanta's 8,000 employees got the word on Tuesday that they had been waiting for: It was O.K. to turn their computers on.

But as the city government's desktops, hard drives and printers flickered back to life for the first time in five days, residents still could not pay their traffic tickets or water bills online, or report potholes or graffiti on a city website. Travelers at the world's busiest airport still could not use the free Wi-Fi.

Ransomware Basics





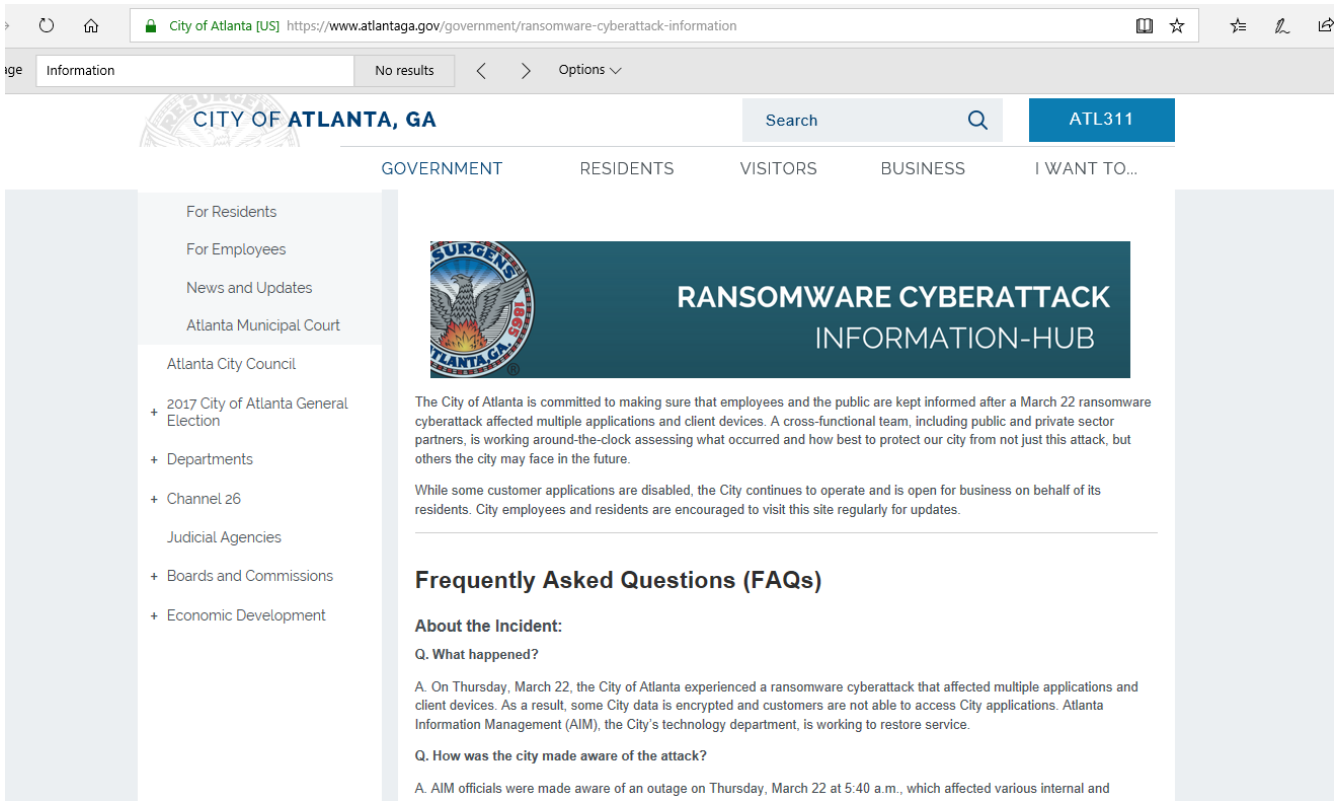
A screenshot of what appeared to be the ransomware affecting systems worldwide on Tuesday. The Ukrainian government posted the shot to its official Facebook page.

March 22, 2018

COA_thisusedtobeyourfile.weapologize

Communication

- Law Enforcement (FBI, DHS, Secret Service)
- City Officials and Employees
- Citizens
  - GA Data Breach Law
- Media



Collaboration

"A cross-functional incident response team"

- Mayor's Office
- City Council
- Atlanta Information Management
- Department of Law
- Department of Procurement
- Department of Finance – Risk Managers
- FBI, Secret Service, Department of Homeland Security
- Private Industry
- EVERYONE

Investigation

- Conduct forensic analysis of systems infected with ransomware to identify:
  - Initial infection vector
  - Potential data exposure
- Perform micro-investigations to determine:
  - Initial access into the environment
  - Impacted systems and user accounts
- Reverse engineer malware to determine the following:
  - Indicators of Compromise (“IOCs”)
  - Ransomware capabilities

Procurement

- The City issued emergency procurements
- Total incident response costs are moving targets
- Maintain complete documentation for future insurance claims

Insurance

- Do you have cyber-insurance.
- What type of claims are covered.
- How do you file a claim.
- Maximizing your recovery.

Best Practices

- Educate employees
- Back up all files (offline & offsite)
- Security patching
- Hire and empower a Chief Information Security Officer
- Strong passwords
- Cyber Insurance
- Segmentation
- Communicate- But Not Too Much!!
- Check employee references/ issue specific levels of clearance and/or access
- Incident awareness/response plan – Emergency response planning
- Prioritize Information Technology funding
- Data audit/ Risk Analysis / Maturity Assessment
- Document/Plan/Be Nimble/Clear Processes

Questions?