SECURITY BRIEF

CITIES UNDER ATTACK: RANSOMWARE CONTINUES TO PLAGUE PUBLIC INSTITUTIONS

The city of Baltimore fell victim to a ransomware attack on May 7, 2019 – the second successful attack in the last year. When the ransomware was discovered, the city notified the FBI and took systems offline to keep the attack from spreading. Unfortunately, the city was unable to react swiftly enough to prevent the majority of city servers from being affected, including systems that enable services like voice mail, email, parking fines, water bills, property taxes, vehicle citations and home sales.

Unfortunately, this isn't an isolated incident. Lynn, Massachusetts and Cartersville, Georgia had payment systems that supported parking tickets and utility services taken offline earlier this month. Additionally, Greenville, North Carolina also was hit by the same ransomware variant that took systems offline in Baltimore: RobbinHood.

ROBBINHOOD RANSOMWARE

The ransomware that infected both Baltimore and Greenville is a new variant of the RobbinHood family that has emerged in the last month. Researchers believe that this was a multi-stage attack, with attackers moving laterally from system to system once access the network has been gained. The malware is then saved on each computer, along with a public key required for execution. Before encrypting data, the ransomware shuts down a range of services including connections to shared network directories and malware-protection tools and backup agents.[1]

It's not clear how hackers gained access to the network, but researchers don't believe that RobbinHood is being spread disseminated through spam. Instead, they are looking at remote desktop services and Trojans as possible culprits.[2]

CONTINUED VULNERABILITY THROUGHOUT PUBLIC INSTITUTIONS

As Baltimore continues to recover from the attack, other states and municipalities may be next on the list of easy targets. Despite ongoing reports of public institutions being affected by ransomware, they are often slow to respond with even basic precautions.

Researchers have found that there are thousands of internet-connected systems that appear to be vulnerable to known issues and exploits, despite warnings dating back to the WannaCry ransomware outbreak two years ago. These networks include many large public school districts.[3]

TAKING PRECAUTIONS

Fortunately, there are some steps that public institutions can take, even if they are strapped for resources and time.

- **Keep systems up-to-date** - Having a plan for maintaining systems is critical to take advantage of the security updates that are included in the latest software updates.

- **Perform regular backups** - Make sure they are encrypted and stored offline. Maintain a 3-2-1 strategy with 3 copies: 2 stored locally and 1 stored offsite.
- **Layer your approach to security** - The most effective security includes protections at both the gateway to the internet (firewall/router) and at the endpoints (antivirus on every device).

While nothing is foolproof, creating a culture of cybersecurity awareness in conjunction with IT protocols can help. If a breach does occur, paying the ransom won't guarantee that files will be decrypted or systems returned to their previous state. With ransomware, an ounce of prevention is worth a pound of cure.

HOW UNTANGLE CAN HELP

Comprehensive protection at the gateway is a key component to any cybersecurity strategy. Untangle's NG Firewall is designed to protect organizations from internet-borne threats like ransomware with a solution that is easy to deploy and manage.

Public sector organizations rely on Untangle to help them safeguard their systems and data. Contact us today to learn more.

Untangle, Inc.
25 Metro Drive, Ste. 210
San Jose, CA 95110
www.untangle.com

ABOUT US

Untangle is the most trusted name in solutions specifically designed to help small-to-medium businesses and distributed enterprises optimize their networks while safeguarding their data and devices. Untangle's Network Security Framework provides cloud-managed security and connectivity options that work together seamlessly to ensure protection, monitoring, and control across the entire digital attack surface from headquarters to the network edge. Untangle's award-winning products are trusted by over 40,000 customers and protect millions of people and their devices. Untangle is committed to bringing open, innovative and interoperable solutions to its customers through its rapidly growing ecosystem of technology, managed services, and distribution partners worldwide. Untangle is headquartered in San Jose, California.

For sales information, please contact us by phone in the US at +1 (866) 233-2296 or via e-mail at sales@untangle.com.

SOURCES

1 https://arstechnica.com/information-technology/2019/05/baltimore-city-government-hit-by-robbinhood-ransomware/
2 https://www.bleepingcomputer.com/news/security/a-closer-look-at-the-robbinhood-ransomware/
3 https://arstechnica.com/information-technology/2019/05/two-years-after-wannacry-us-schools-still-vulnerable-to-eternalblue/
– https://www.witn.com/content/news/Greenville-city-computers-shut-down-after-virus-attack-508373251.html
– https://www.mdjonline.com/neighbor_newspapers/west_georgia/news/cartersville-working-with-authorities-after-ransomware-attack-shuts-down-online/article_07c5d9ce-700c-11e9-871b-9b9f0c5ad9e3.html
– https://www.baltimoresun.com/news/maryland/politics/bs-md-ci-it-outage-20190507-story.html