WaterISAC Advisory on Current Egregor Ransomware Incident at Large Metropolitan Water Utility

Friday, October 30, 2020

This advisory is marked TLP:GREEN. See definition below.

WaterISAC is aware that a large metropolitan water utility is currently dealing with an Egregor ransomware incident. While the incident response is ongoing, the utility asked us to publish an advisory to members for broader sector awareness so everyone can take necessary actions to address this virulent threat.

What happened?

- The Egregor ransomware executed early Thursday morning.
- The initial infection vector was potentially a macro-enabled document attachment containing Qakbot – Qakbot is widely utilized to distribute ransomware payloads.
- After the initial infection, the threat actors leveraged RDP (remote desktop protocol) to traverse network resources.
- Thus far, over one hundred workstations and multiple servers, including a backup server have been impacted – the utility wishes to stress that the backup servers were targeted, making it imperative to have a robust and resilient backup strategy.
- The ransom note does threaten data leakage, and forensic reviews show definite attempts via FTP to steal files. Whether or not the actors were successful in exfiltrating data is unknown at this time.
- Furthermore, the utility urges members to enable deep packet inspection on firewalls for maximum effectiveness in detecting this threat.

Recommended actions to take immediately

WaterISAC continues reminding members to plan/prepare for the worst and hope for the best. When it comes to ransomware, regularly:

- Revisit, review, and discuss ransomware and data breach playbooks/policies/procedures, and keep them up-to-date. The CISA/MS-ISAC Ransomware Guide is a valuable resource to be used for prevention and response best practice guidance.
- Keep a reputable incident response firm on retainer before an incident occurs.
- Evaluate cyber insurance policies to confirm proper coverage.
- Send out security awareness reminders to all staff on how phishing is a very common initial infection vector for ransomware.

- Remind staff not to open attachments or click on links contained in emails, even if the email looks like it is from a trustworthy source. And if they already have received and/or actioned a suspicious email, encourage them to report the event now.
- Check device and network logs and events for potential intrusions, and consider configuring alerts for changes to files.
- Test backups and restore procedures before you need them and make sure you have a valid tested copy stored offline.
- Report ransomware incidents to authorities (and WaterISAC).

Additional resources on Egregor ransomware

- https://threatpost.com/egregor-ransomware-mass-media-corporate-data/159816/
- https://www.darkreading.com/vulnerabilities---threats/meet-egregor-a-new-ransomware-family-to-watch/d/d-id/1339091

For questions and to report incidents, email analyst@waterisac.org.

Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community. Visit https://www.cisa.gov/tlp for more information.