Wisconsin DOJ: AG Kaul warns Wisconsinites of increase in ransomware threats

Posted on Monday, Sep 13, 2021

Contact: DOJCommunications@doj.state.wi.us

MADISON, Wis. – Attorney General Josh Kaul is advising Wisconsinites to be aware of ever-evolving ransomware threats. The COVID-19 health crisis has increased online dependence, which has increased the chance of Wisconsinite exposure to cybersecurity crimes. To date, the FBI has received 41 ransomware reports in Wisconsin this year, compared to 30 reports total in 2020.

“As technological threats continue to evolve and become more sophisticated, DOJ’s Cyber Unit remains committed to investigating cybercrimes throughout Wisconsin,” said Attorney General Kaul. “All of us can help combat the threat of ransomware by taking a few precautions: not clicking on links or attachments from unverified sources, using unique, complex passwords, and installing computer updates regularly.”

Ransomware is a type of malicious software cyber actors use to deny access to systems or data.[1] The malicious cyber actor holds systems or data hostage until the ransom is paid. After the initial infection, the ransomware attempts to spread to shared storage drives and other accessible systems. If the demands are not met, the system or encrypted data remains unavailable.

A person may unknowingly download ransomware onto a computer by executing one of the following actions embedded with malware: opening an email attachment, clicking an advertisement, following a link, or visiting a website. Cyber actors continue to evolve their ransomware tactics over time to extort organizations and

citizens. Awareness of these tactics is important to avoid unnecessary exposure.

Better defense equals better offense

Cyber-attacks may be prevented by following the Department of Homeland Security – Cybersecurity and Infrastructure Security Agency (CISA) best practices for managing risks posed by ransomware: https://www.cisa.gov/stopransomware

Apply these practices to the greatest extent possible based on availability of resources:

- Keep an offline backup of your files
- Avoid unfamiliar contact through emails, links, advertisements, websites, text messages, etc.

To learn more, visit the CISA Ransomware Guide at, https://www.cisa.gov/sites/-default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf

When in doubt, report it out

Victims of ransomware attacks are encouraged to resist any urge to fulfill a ransom request. Compliance in response to a ransom does not guarantee the captured data will be returned. Compliance also encourages perpetrators to target more victims and offers an incentive for other cyber actors to get involved in this type of illegal activity.

If you believe you are a victim of a ransomware attack:

- Contact Wisconsin DOJ's Cyber Unit https://wifusion.widoj.gov/
- Contact your local Federal Bureau of Investigation Field Office (FBI) https://www.ic3.gov/

---

[1] Ransomware: What It Is and What To Do About It (justice.gov)