



COT Security Alert – KULUOZ Botnet

A recent increase in attempts to infect state users with the KULUOZ botnet has been observed. A botnet is used by cybercriminals to distribute malware broadly and effectively, since infected devices become part of the botnet when they are used in further attacks. The method used to spread the KULUOZ botnet has been to attach infected files to spam emails. The spam emails use social engineering tactics to entice users to click attachments in the email, which also downloads the malicious code without the user's knowledge. The emails most often appear to come from legitimate sources such as FedEx, USPS, Delta, American Airlines or the IRS luring users to open a familiar type of attached document such as .PDF or .DOC.

COT Security staff are monitoring and using the security tools in place to protect the state network; however, users may still become infected if a malicious file is opened. Attackers change techniques often to avoid detection.

Users are advised never to open attachments in unexpected emails, even when the sender is known or the email appears to come from a trusted source without first contacting the known sender or trusted source contact for verification.

NOTICE: COT is providing this information so that you are aware of the latest security threats, vulnerabilities, software patches, etc. You should consult with your network administrator or other technical resources to ensure that the appropriate actions for these alerts are followed. If you are a network administrator and need additional information, please call the Help Desk at 502.564.7576.

Office of Chief Information Security Officer
Commonwealth Office of Technology
Frankfort, KY 40601
technology.ky.gov

Technology-enabled Business Solutions for 21st Century Government