Colonial Pipeline CEO to testify on Capitol Hill in June following cyberattack

Colonial Pipeline CEO Joseph Blount will testify in June before the House Homeland Security Committee at a hearing one month after the company was forced to shut down operations due to a devastating ransomware attack.

The hearing, which will take place June 9, will focus on the pipeline attack, which resulted in gas shortages in several U.S. states, as well as how to strengthen critical infrastructure.

The pipeline provides around 45 percent of the East Coast’s fuel. Operations were disrupted after the ransomware attack on the company’s IT system forced the company to shut down the pipeline for almost a week to protect operational controls.

The RSA breach, when it became public days later, would redefine the cybersecurity landscape. The company's nightmare was a wake-up call not only for the information security industry—the worst-ever [crack] of a cybersecurity firm to date—but also a warning to the rest of the world. Timo Hirvonen, a researcher at security firm F-Secure, which published an outside analysis of the breach, saw it as a disturbing demonstration of the growing threat posed by a new class of state-sponsored [attackers]. “If a security company like RSA cannot protect itself, how can the rest of the world??

The question was quite literal. The theft of the company’s seed values meant that a critical safeguard had been removed from thousands of its customers’ networks. RSA’s SecurID tokens were designed so that institutions from banks to the Pentagon could demand a second
form of authentication from their employees and customers beyond a username and password? something physical in their pocket that they could prove they possessed, thus proving their identity. Only after typing in the code that appeared on their SecurID token (a code that typically changed every 60 seconds) could they gain access to their account.

- **How to Tell a Job Offer from an ID Theft Trap [4]**

  One of the oldest scams around — the fake job interview that seeks only to harvest your personal and financial data — is on the rise, the FBI warns. Here’s the story of a recent LinkedIn impersonation scam that led to more than 100 people getting duped, and one almost-victim who decided the job offer was too-good-to-be-true.

- **Fork Brute Force Attack Detection/Mitigation Still Being Worked On For The Linux Kernel [5]**

  A security module continues to be worked on for being able to detect and mitigate against fork/execute brute force attacks to Linux systems.

  The latest iteration of patches to be able to provide brute force attack mitigation against fork/exec abuse was sent out on Friday. This seventh spin on the patches reworks some of its tracking of statistical data and other improvements. See the earlier work on this Linux Security Module (LSM) covered in Linux Patches Aim To Provide Fork'ing Brute Force Attack Mitigation.

---

**Security**

Source URL: [http://www.tuxmachines.org/node/151483](http://www.tuxmachines.org/node/151483)

Links: