The Week in Security: A possible Colonial Pipeline 2.0, ransomware takes bite out of American eateries | ReversingLabs

By Carolynn van Arsdale, Writer, ReversingLabs.Carolynn van Arsdale

Published: 2023-04-27 · Archived: 2026-04-05 13:31:43 UTC

Security OperationsApril 27, 2023

Welcome to the latest edition of The Week in Security, which brings you the newest headlines from both the world and our team across the full stack of security: application security, cybersecurity, and beyond.

This week: A Canada gas pipeline could have suffered an explosion caused by a cyber attack. Also: Financial services firm NCR hit with a ransomware attack, hurting thousands of small American eateries.

This Week's Top Story

Possible Colonial Pipeline 2.0? Security incident causes concern for Canada's critical infrastructure

A Canadian gas pipeline suffered a security incident that could have caused an explosion at the company's gas site, according to a New York Times story that cited leaked U.S. intelligence documents. The attackers, from a the pro-Russia hacking group Zarya, were communicating with Russia's Federal Security Service (FSB), the primary successor to the KGB, about the incident's potential for physical damage, according to the leaked documents.

Canadian Prime Minister Justin Trudeau confirmed that the unnamed Canadian gas pipeline was attacked, but said there had been no physical damage to any of Canada's energy infrastructure. The cyber attack which took place on February 25, 2023, was intended to economically damage the company. With respect to the possibility of physical damage, Zarya had access to the infrastructure of the gas pipeline operator, and was awaiting further instructions from Russian intelligence on how to proceed.

This incident is alarming for two reasons. First, the attack demonstrates that pro-Russian threat actors can penetrate the critical infrastructure systems of Western countries. Second, communications between Zarya and Russian intelligence demonstrate that pro-Russian hacking groups could be operating and taking direction from the Russian government, which means that this incident could have been carried out based on nation-state adversary's motivations.

News Roundup

Here are the stories we're paying attention to this week…

Financial services firm NCR hit by ransomware attack, disrupting Aloha and Back Office products (CPO Magazine)

A payment processing system used by over 100,000 restaurants and bars has been temporarily disrupted as its parent company, NCR, has been hit with a ransomware attack. Most affected are independent eateries and small local chains across the U.S.

GitLab's new security feature uses AI to explain vulnerabilities to developers (TechCrunch)

Developer platform GitLab today announced a new AI-driven security feature that uses a large language model to explain potential vulnerabilities to developers, and it plans to expand on this feature in the future to automatically resolve those vulnerabilities using AI.

Linux shift: Chinese APT Alloy Taurus is back with retooling (Dark Reading)

After a brief hiatus, the Alloy Taurus APT (aka Gallium or Operation Soft Cell) is back on the scene, with a new Linux variant of its PingPull malware. The Chinese nation-state-affiliated threat actor has been around since at least 2012, but has only been in the spotlight since 2019. It focuses on espionage, and tends to target major telecommunications providers.

#RSAC: Election protection is CISA's top priority for next 18 months (InfoSecurity Magazine)

For CISA, the protection of the looming 2024 election is now a high priority in its effort to protect democracy: "This is our top priority over the next year and a half," says Eric Goldstein, executive assistant director for cybersecurity at CISA.

U.S. Cyber Command is sending experts abroad to help allies catch hackers (Tech Monitor)

The U.S. government's Cyber National Command Force (CNCF) is sending its experts abroad in so-called "hunt-forward" operations to aid partner countries in combating cybercrime. It has launched 47 operations in 20 countries over the last three years.
