Coalfire Labs Develops Open Source Password Cracking Tool

"NPK" Tool Provides Unprecedented, More Affordable Password Cracking Power to Security Professionals

Westminster, CO – March 21, 2019 – Coalfire, a trusted provider of cybersecurity advisory and assessment services, announced today that the Coalfire Labs Research and Development (R&D) team released NPK, an open source tool that provides unprecedented password cracking capabilities to break the security surrounding hashed passwords.

The distributed hash-cracking platform is built entirely of serverless components in Amazon Web Services (AWS) including Cognito, DynamoDB, and S3. It leverages the exceptionally powerful GPU instances in AWS to bring staggering hash cracking performance to a price tier in reach of a weekend tinkerer. It was designed for easy deployment and flexible usage.

"Let's face it: even the most comprehensive cracking rig spends a lot of time at idle," said Brad Woodward, Director, Coalfire Labs, and developer of the tool. "NPK lets you leverage extremely powerful hash cracking with the 'pay-as-you-go' benefits of AWS."

It's not uncommon for a penetration test to hinge on recovering a plaintext password from one of these hashes. Whether it's NTLM hashes from Active Directory, NetNTLMv2 from Responder, WPA2 PMK from a wireless penetration test, or hundreds of other possible sources of hashes, recovering the original password has been a challenge for hackers for decades. Unlike encryption, hashing isn't reversible.

The only way to "recover" the password from the hash is to guess what the password is, run it through the hashing algorithm, and see if the result matches the hash you have. For security professionals, the biggest challenge isn't the software – it's the hardware: hardware, electricity, and maintenance of password hashing "rigs" often run in the tens of thousands of dollars per year, taking them out of range of many budget-constrained security operations teams and penetration testing enthusiasts.

NPK features include:

- Very easy installation – One config file and one command to run.
- Intuitive campaign builder – Take the trial and error out of complex attack types with the intuitive campaign builder. With a couple of clicks, users can create advanced campaigns that even advanced password cracking users would struggle to emulate.
- Campaign price and coverage estimation – Take the guesswork out of your campaigns. See how far you'll get and how much it will cost *before* starting the campaign.
- Multi-tenancy and data lifecycle management – Ensure that passwords don't get leaked and data remains properly segmented. Campaign cleanup is automatic.

NPK is an acronym for the three primary atomic elements in fertilizer (nitrogen, phosphorous, and potassium), which are designed to increase your crop yield; like fertilizer, NPK increases your crop of cracked credentials at a significantly lower cost than any solution available today, bringing fast, high-volume password cracking into reach of the broader penetration testing community.

Resources:

- https://github.com/Coalfire-Research/npk

About Coalfire

Coalfire is the trusted cybersecurity advisor that helps private and public-sector organizations avert threats, close gaps and effectively manage risk. By providing independent and tailored advice, assessments, technical testing and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives and fuel their continued success. Coalfire has been a cybersecurity thought leader for more than 17 years and has offices throughout the United States and Europe.

For more information, visit Coalfire.com.

Press Contact:
Mike Gallo
For Coalfire
212-239-8594
Luminacoalfire@luminapr.com