COALFIRE
Cybersecurity that fuels success

Coalfire Labs R&D Team Releases Icebreaker Tool

Open Source Tool Automatically Captures Active Directory Credentials, Improving Efficiency for Security Professionals

Westminster, CO – March 15, 2018 – Coalfire, a trusted provider of cybersecurity advisory services, announced today that the Coalfire Labs R&D team released Icebreaker, an open source tool that captures Active Directory credentials automatically.

Icebreaker helps security professionals automate network attacks against Active Directory from a position inside the network but outside of Active Directory, providing them with plaintext credentials. Authored by Coalfire Senior Security Consultant Dan McInerney, Icebreaker automatically performs five different network attacks in sequence to capture plaintext credentials and hashes. Attack types include:

- **Reverse Bruteforce:** Uses several techniques to find valid and potentially valid domain usernames, which are tested against two of the most common Active Directory passwords.
- **Malicious file upload:** Writes a malicious SCF to available network shares that, when opened in explorer by domain users, will send their password hash to the attacker.
- **Broadcast protocol poisoning:** Poisons layer two broadcast protocols to trick domain users' machines into sending their password hash to the attacker.
- **SMB relay:** Man-in-the-middle attacks SMB connections to gain remote code execution against victim machines. Icebreaker will add a new administrative user to the machine as well as run and parse Mimikatz on it.
- **IPv6 DNS poison:** Poisons IPv6 DNS requests to trick users' browsers into sending their password hash to the attacker.

Resources:

- Icebreaker: https://github.com/danmcinerney/icebreaker

"By automating what was once a very lengthy, manual and time-intensive process, Icebreaker enables Coalfire to improve the speed, efficiency and effectiveness of internal network testing for its own clients, while also delivering this open source capability to security teams within organizations to help them improve their security posture," said McInerney.

Hashes captured by the Icebreaker tool are autocracked, leveraging both the JohnTheRipper password cracker utility and a Coalfire-customized 1 million password wordlist built specifically for Active Directory passwords.

Icebreaker also includes the option to kick off Empire and DeathStar upon a successful SMB hash relay in order to gain automated domain admin rights.

About Coalfire

Coalfire is the 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 16 years and has offices throughout the United States and Europe.

For more information, visit Coalfire.com.

COALFIRE
Cybersecurity that fuels success

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