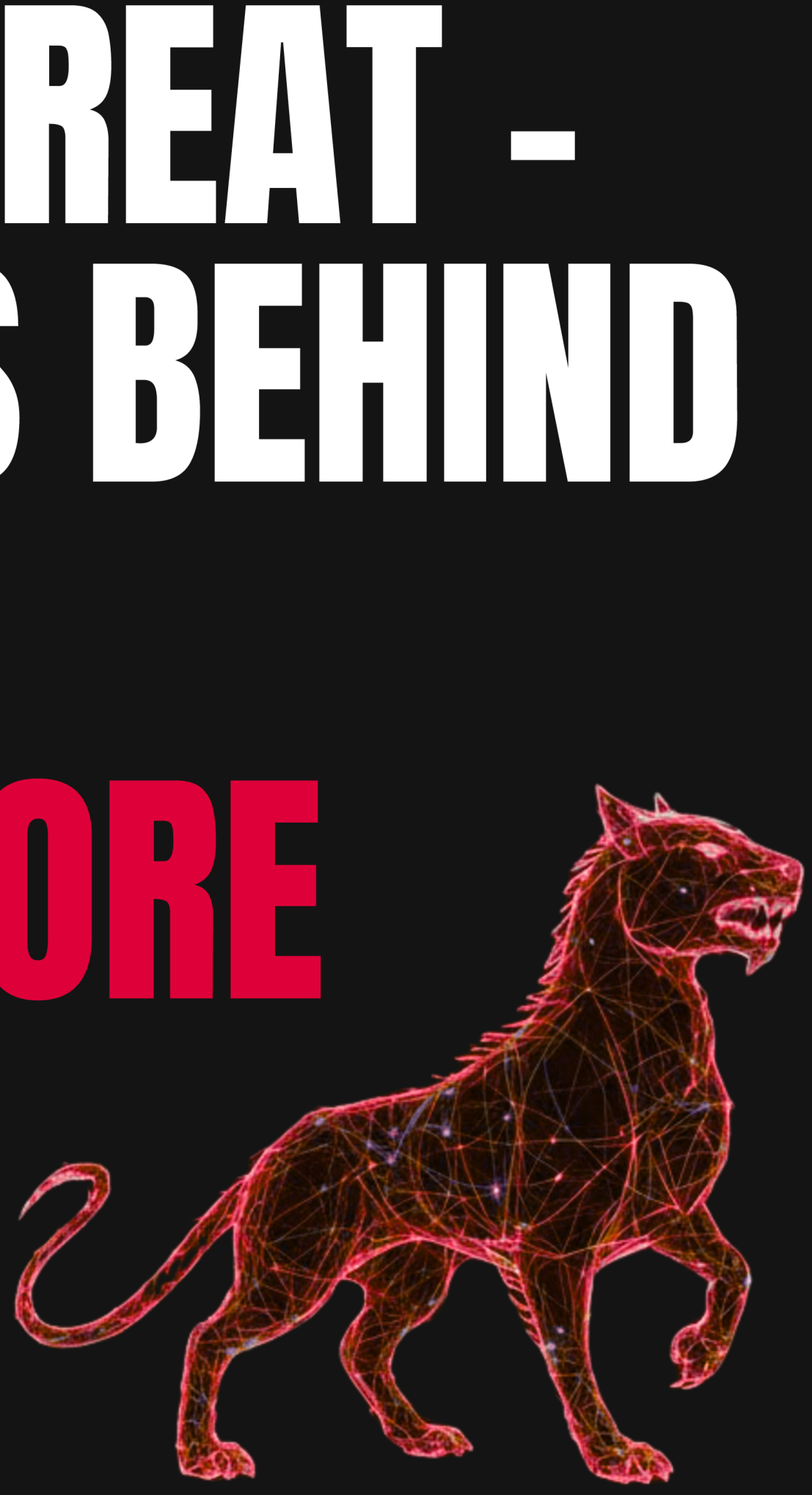
breachsimrange

FAKE JOBS AND REAL THREAT - WHAT IS BEHIND NIMBUS MANTICORE



BREACHSIMRANGE.IO

breachsimrange

WHO IS NIMBUS MANTICORE?

Nimbus Manticore is a highly sophisticated threat actor group, assumed to be aligned with Iranian state interests, that focuses on the defense, aerospace, and telecommunications sectors across Europe and the Middle East.

The group has drawn attention for its realistic social-engineering strategies, primarily involving fake job offers designed to impersonate recruiters from reputable companies.

They are known for exploiting Windows DLL sideloading flaws to silently establish access within targeted systems, allowing attackers to execute malicious code through legitimate signed executables. Once inside, the actor deploys custom malware (MiniJunk and MiniBrowse), and persists quietly to steal sensitive data.

BREACHSIMRANGE.IO

breachsimrange

INSIDE THE ATTACK CHAIN

Reconnaissance

Identify key employees (HR, engineers)

Fake Job Portal

Email lures with career-site clones

Download / delivery

Contains legitimate EXE + malicious DLL

Run the Installer (EXE)

Victim runs legitimate EXE, triggering malicious DLL load.

DLL Side-Loading

Malicious DLL executes within trusted process

Payload Activation

MiniJunk (backdoor) / MiniBrowse (stealer)

Persistence and Evasion

Scheduled tasks, obfuscation, code signing

C2 and Exfiltration

Data sent to attacker infrastructure (HTTPS/CDNs)

BREACHSIMRANGE.IO

MALWARE SNAPSHOTS

MiniJunk (Backdoor)

- Remote control and file operations
- Plugin system for custom modules
- Obfuscated code and persistence via %AppData%
- Signed with stolen certificates

MiniBrowse (Stealer)

- Extracts credentials from browsers
- Collects system IDs and user info
- Uses named pipes for communication
- Exfiltrates data in JSON over HTTPS

IMPACT BEYOND PROFIT

Nimbus Manticore's campaigns seems to be aligned with Iranian strategic interests - intelligence gathering, defense research theft, and geopolitical influence.

- ☐ Theft of intellectual property and sensitive R&D data
- ☐ Credential compromise enabling deeper network access
- ☐ Long-term espionage and supply-chain infiltration
- ☐ Strategic intelligence advantage for state interests

DEFENSE RECOMMENDATIONS

Phishing

Train employees to identify phishing emails. Deploy proper security controls

Downloads

Strengthen EDR to detect malicious ZIPs and installers

Endpoint Security

Create detection rules for DLL side-loading based on Nimbus Manticore’s activity

Access Control

Enforce least privilege and use application allow-listing

Threat Intel

Continuously track threat intel updates

KEY TAKEAWAYS

Nimbus Manticore's blend of human deception and technical sophistication shows how modern APTs pursue influence over notoriety.

Defenders must combine technical visibility, continuous threat intel, and informed human vigilance.

Understanding attacker motivation and persistence patterns is crucial for proactive defense and incident response planning.

Integrating people, processes, and technology strengthens detection, mitigates lateral movement, and reduces social engineering exposure.

breachsimrange

Contact us for emulating sophisticated adversaries and threat actor groups in your organization, performing offensive security consulting, and assessing your cyber defense posture.

✉ ops@breachsimrange.io

BREACHSIMRANGE.IO