Intersection of Geopolitics and Credential-Based Threats

October 8, 2025

Stephanie Schneider
Cyber Threat Intelligence Analyst,
LastPass

Contents

What is CTI?

Cyber Threat Intelligence (CTI)

Cyber threat intelligence is the broad field of collecting and analyzing data to understand threats.

- Threats = intent + capability
- Intelligence = analyzed information to add relevant insights

Source: Cyber Security Services, Accreditations & Training (CREST)

Strategic Cyber Threat Intelligence

Strategic CTI seeks to provide high-level insights to decision makers by using

- Geopolitical context
- Industry trends
- Potential consequences

How can CTI benefit me?

Applying intelligence-driven insights into practice

Proactive threat prioritization

Provides an early warning against a range of advanced threats

Informed decision-making

Make decisions based on the larger cyber threat environment

Strategic alignment

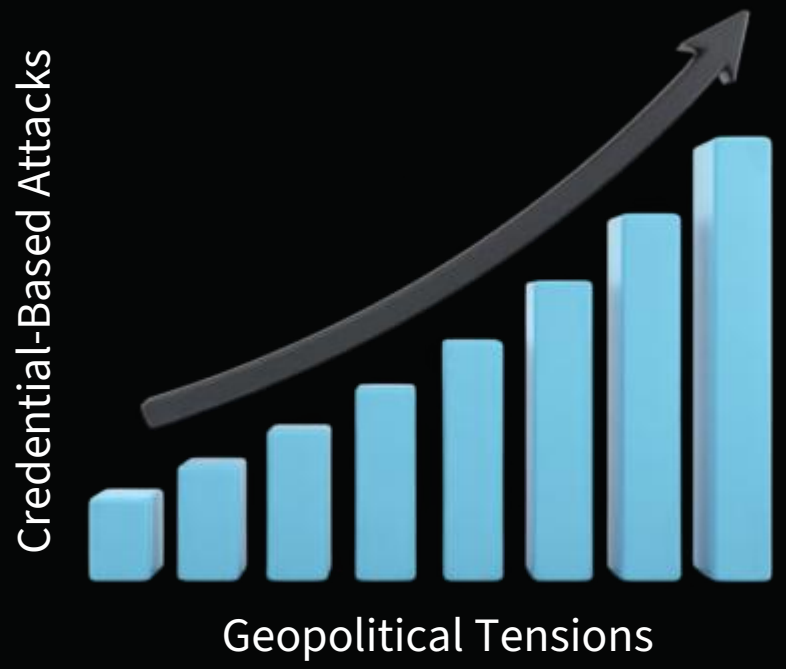
Make decisions based on the larger cyber threat environment

Efficient resource allocation

Prioritize security investments

Geopolitical tensions x credential-based attacks

As global tensions rise, businesses must treat identity security as a frontline defense.



- Credential stuffing
- Phishing, social engineering
- Cloud credential abuse
- Living off the Land (LOTL)

- Credential-based attacks pose a serious threat, particularly in the context of geopolitical events.
- Credentials provide adversaries with the initial access needed to launch various malicious activities:
  - Espionage, sabotage, or financial gain

Geopolitics: a driving force for credential-based attacks

Geopolitical tensions contribute to an increase in credential attacks and other forms of cyber warfare, reflecting a broader shift towards digital conflict as an extension of international relations.

- **Cyberwarfare as an extension of geopolitics**
  - Geopolitical tensions often lead to increased cyber warfare activity → attacks on critical infrastructure, government entities, and private businesses to gain strategic advantages or disrupt adversaries.
- **Credential attacks are a preferred vector**
  - Many state-sponsored and politically-motivated attacks use stolen credentials to gain unauthorized access.
  - According to CISA, over 50% of attacks on government and critical infrastructure exploit valid credentials.
- **Motivation and opportunity**
  - Geopolitical tensions increase the motivation for cyberattacks.
  - The prevalence of stolen credentials from previous breaches provides a ready supply for attackers.
- **Hybrid warfare**
  - Cyberattacks are often used in conjunction with conventional military operations and disinformation campaigns as part of hybrid warfare strategies.

Infostealers driving credential theft

Nation-state groups and other groups benefit from the vast, growing market for infostealer logs.

- Infostealers stole 2.1B (75%) of 3.2 billion stolen creds.
- 69% of infostealer infections impacted corporate hosts and devices; 21.3% affecting small biz.
- Infostealers drove nearly a quarter (24%) of all cyber incidents in 2024, according to Huntress.
  - 104% YoY increase in infostealer detections, with SMBs hit hardest due to limited resources.
- Nation-state groups use credentials obtained from infostealer malware logs distributed via:
  - Dark web marketplaces
  - Telegram channels that sell logs from malware like RedLine, Raccoon Stealer, and Vidar

Impact of credential-based attacks

Disruption & destruction

Critical infrastructure is a common target.

- Credential theft can grant access to systems that control critical infrastructure, leading to disruptions of essential services.

Espionage & data theft

- **Stolen credentials enable access to sensitive information.**
- Allows adversaries to steal valuable data, intellectual property, or confidential intelligence.

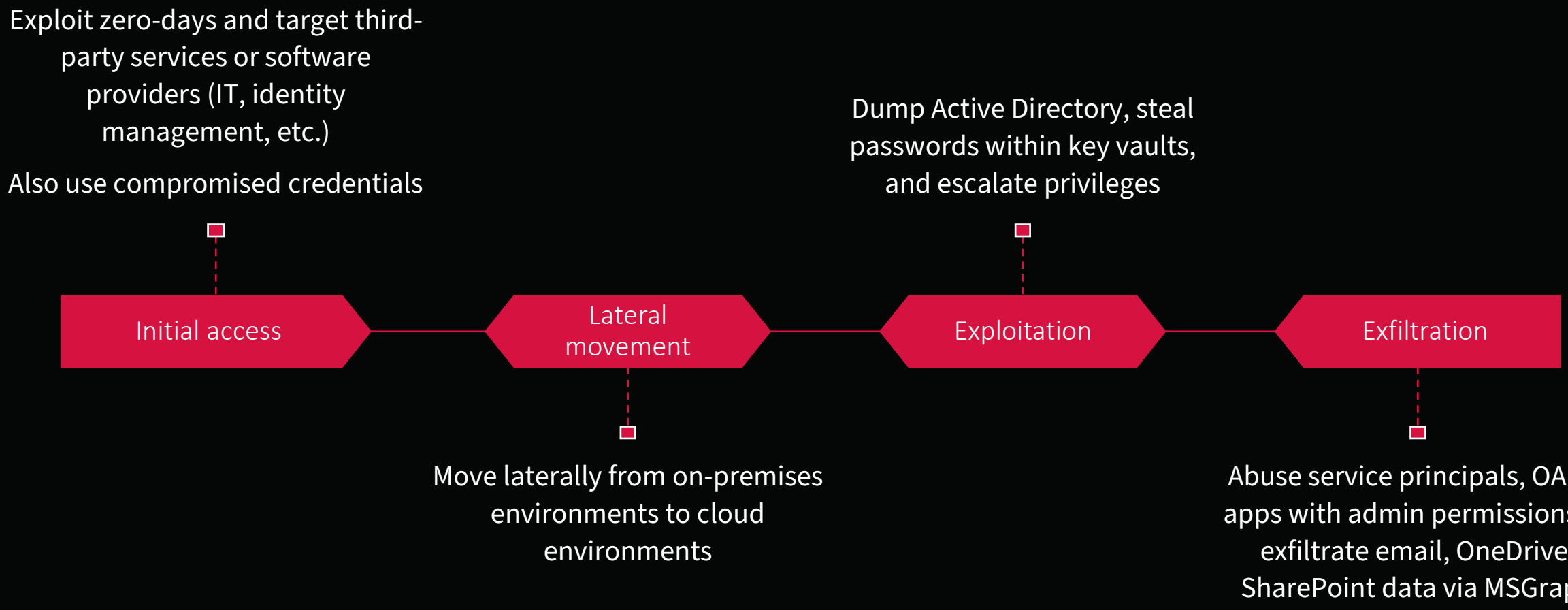
Financial gain or economic instability

- **Attacks on financial institutions and critical third-party providers can pose systemic risks to financial stability.**
  - Can lead to financial losses, business disruption, and erosion of public trust in institutions.

Case Studies

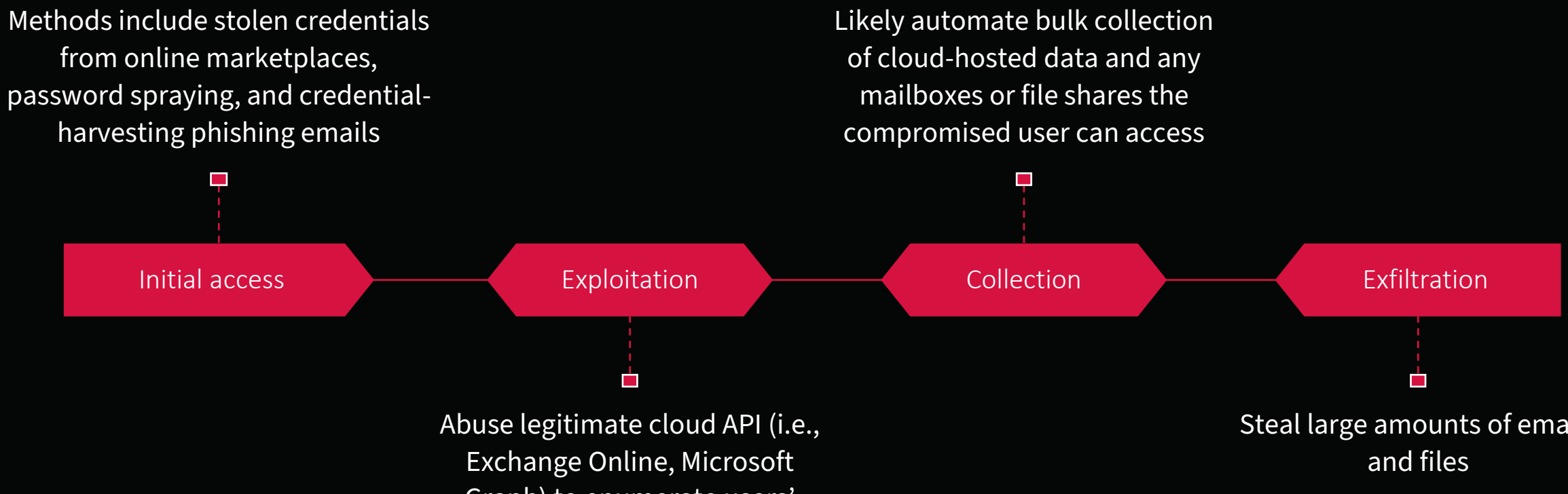
Case Study: Chinese supply chain compromise

Silk Typhoon is targeting remote management tools and cloud services in supply chain attacks that give them access to downstream customers. The group has shifted from primarily using zero-day vulnerabilities to abusing stolen API keys and compromised credentials.



Case Study: Void Blizzard leverages stolen creds

Void Blizzard is conducting espionage operations primarily targeting organizations considered important to Russian government objectives. These attacks often use stolen credentials likely purchased from online marketplaces to gain access.



Outlook

In conclusion, the nexus between geopolitical tensions and credential-based attacks is undeniable and continues to grow. As global conflicts persist, the cyber landscape will likely remain a critical battleground, with credential compromise serving as a favored tactic for achieving strategic objectives.

The escalation of geopolitical tensions has several broader implications for credential-based attacks.

AI Integration

- The expanding digital attack surface, coupled with advancements in AI, further exacerbates the threat.
- AI is increasingly used to make more convincing phishing attacks and automate credential stuffing, making these attacks harder to detect and defend against.
    - i.e., Fraud-as-a-Service toolkits can launch large-scale account takeovers that can test millions of stolen credentials per hour

Global Impact and Collateral Damage

- Organizations not directly involved in geopolitical conflicts can still become collateral damage. State-sponsored attacks can disrupt industries and expose critical supply chain vulnerabilities globally.
- This elevated threat environment underscores the critical need for organizations to strengthen their cybersecurity defenses, particularly focusing on identity and access management, which remains a common weak point.


Questions?

Appendix

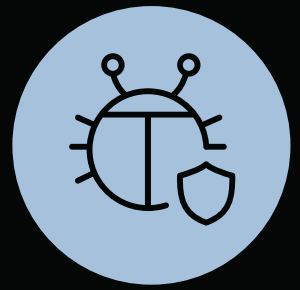
Threat actor motivations

Threat actors are driven by various motivations:

State-sponsored hackers

Rising geopolitical tensions often lead to rise in state-sponsored cyberattacks, including targeting critical infrastructure.

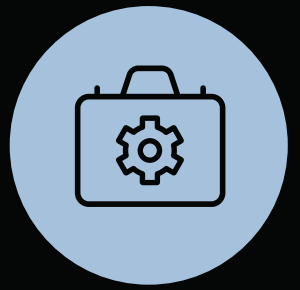
- **Nation-state attacks frequently target credentials to gain initial access and conduct follow-on activities.**



Criminal exploitation

Cybercriminals can exploit instability and major events to launch opportunistic attacks. Some criminal groups may coordinate with or take direction from nation-state actors.

- **They can leverage the increased vulnerability and confusion to conduct malicious activities like financial fraud or data theft.**



Hacktivism

Conflicts and political instability can fuel ideologically-motivated hacktivist groups that sometimes overlap with nation-state actors.

- **These groups often use credential-based attacks, including social engineering and phishing, to gain access to systems and disrupt operations.**

Mitigation recommendations

ZERO TRUST ARCHITECTURE

- Assume breach and verify every access attempt.
- Several foundational components form this architecture to ensure that access to resources is granted only after thorough verification and based on the principle of least privilege.
- These components include identity, devices, network, data, and more.

STRONG PASSWORD POLICIES & MFA

- These are essential to prevent credential misuse.
- Implementing strong password policies and mandating phishing-resistant multi-factor authentication (MFA) (like passkeys) significantly reduces the risk of credential theft and unauthorized access.
- This will add a layer of protection against common credential attacks like password spraying, brute force attacks, and MFA bypass.

THREAT INTELLIGENCE MONITORING & SHARING

- A robust threat intelligence program will help your organization stay ahead of threats.
- Dark web monitoring detects exposed credentials by continuously scanning forums and marketplaces where hackers buy and sell stolen data. This provides an early warning system.
- Cross-sector collaboration to detect and respond to threats is also key.

USER TRAINING & AWARENESS

- Educating employees about social engineering, phishing, and the risks of credential theft is crucial in preventing attacks.

INCIDENT RESPONSE PLANNING

- Include geopolitical escalation scenarios to understand how your organization may be impacted directly or indirectly by an active conflict and how to respond to limit the impact to business operations.