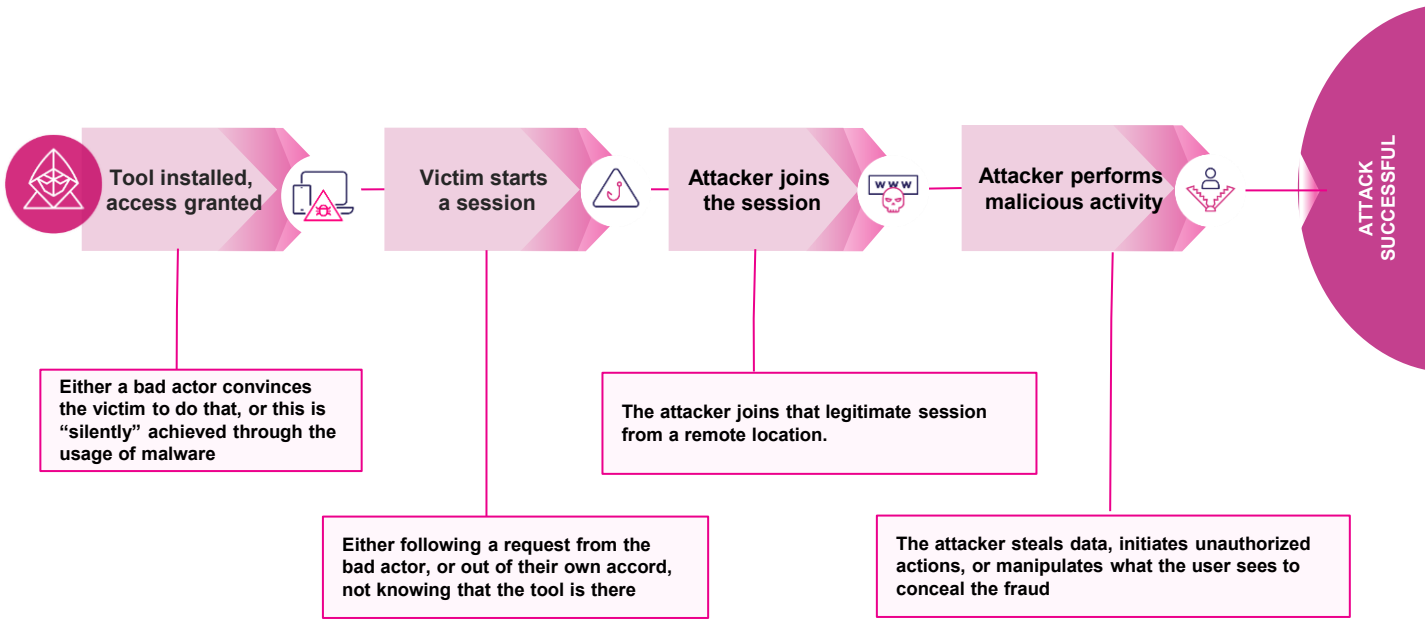
MEMCYCO

Detecting and Disrupting Remote Desktop Takeover in Real Time

Attack anatomy

Remote access scams exploit tools like AnyDesk, TeamViewer, or LogMeIn to run remote sessions on victims' devices. These sessions are hard to detect because they originate from recognized devices, use valid credentials, and involve seemingly legitimate activity.

Attackers often pose as tech support agents or company representatives, cold-calling victims and tricking them into installing remote access tools. They then request access rights, or, in more covert scenarios, malware installs the tool silently, leaving victims unaware their device has been compromised.



User-level exploitation

These scams give attackers covert control of a logged-in user's device, enabling actions such as:

- **Unauthorized fund transfers**
- **Credential theft**
- **Card data harvesting**
- **Theft of PII (e.g., social security number, home address etc.)**

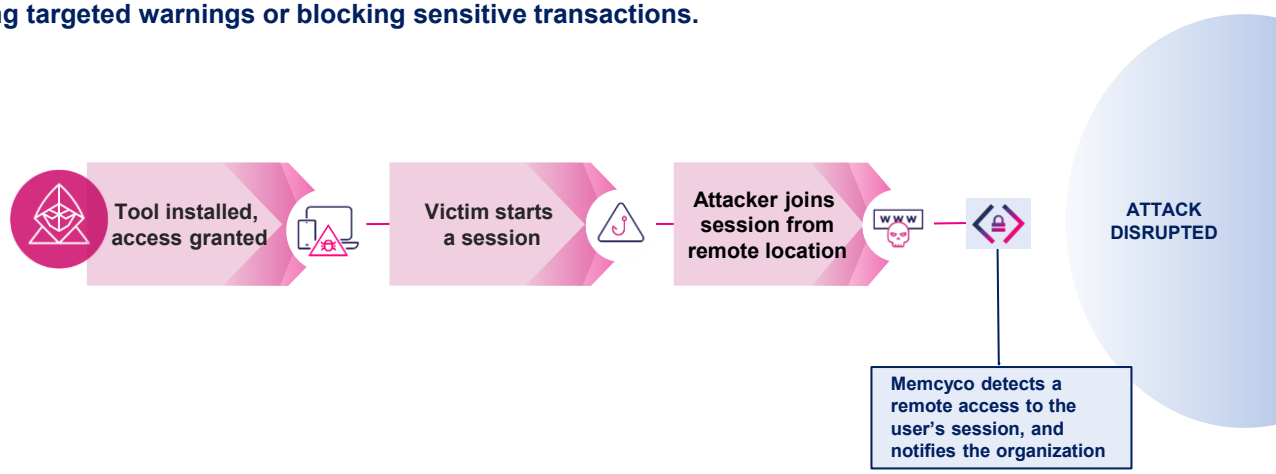
Impact on the organization

- **Increased fraud reimbursements**
- **Regulatory exposure**
- **Reputation damage and erosion of customer trust**

Worse, many victims don't realize they've been compromised until it's too late, leading to complaints long after the attack ends.

Memcyco's solution

Memcyco detects remote sessions in real time and alerts the organization to suspicious activity. The organization can further investigate, and in case of a scam can then trigger protective actions such as displaying targeted warnings or blocking sensitive transactions.



Agentless solution, proven value

Memcyco deploys rapidly with no agents or impact on user experience. It integrates seamlessly into existing security workflows through dashboards and APIs, enabling real-time visibility and automated response for SOC teams.

Organizations see early and measurable ROI, driven by less fraud incidents, fewer support escalations, and stronger digital trust, without disrupting customer journeys or burdening IT operations.

Who we serve, and how they benefit

SECURITY TEAMS

Upgrade security & auditability

- ✓ Cut incident count
- ✓ Reduce OPEX
- ✓ Strengthen compliance
- ✓ Close PII theft gaps

FRAUD TEAMS

Decrease cost and impact of fraud

- ✓ Reduce ATO fraud
- ✓ Lower customer reimbursement
- ✓ Shorten investigation times
- ✓ Improve anti-fraud tools

DIGITAL TEAMS

Grow brand equity and retention

- ✓ Protect Digital Trust
- ✓ Reduce attrition
- ✓ Shield credibility
- ✓ Cut risk of bad PR