Lab work 1- Cyber Threat Intelligence report mapping to Tactics and Technics

Names:
Adi Haim
Afik Aharon
Bar Mor
Ron Noiman

Source CTI report:
https://cloud.google.com/blog/topics/threat-intelligence/voice-phishing-data-extortion

The report investigates a voice phishing campaign conducted by threat actors known as shinyhunters, that impersonated IT support personnel to gain access to internal systems. the attackers use something called phone based social engineering to trick employees to sharing credentials or approving MFA requests. once credentials are obtained, they log into corporate networks, remove sensitive data, and extort victims by threatening data leaks they found.

The GTIG(Google's Threat Intelligence Group) links this activity (written above) to a financially motivated group called UNC6040. Instead of stealing passwords, this group convinces victims to authorize a malicious salesforce connected app. With that access they extract personal data from the CRM database and later use it to extort organizations. Sometimes even months after the initial breach, other similar groups may follow up with ransom demands.

Attack Flow- Schema:

Reconnaissance: targeted specific employees, often within English-speaking branches of multinational corporations without gathering personal data beforehand technique- voice phishing

The attacker is requesting the user credentials. Reconnaissance - T1589.001 (Gather Victim Identity Information: Credentials)

Initial Access: call employees pretending to be IT staff and convince them to visit a fake login page or an approved MFA prompt. technique- phishing, valid Accounts. For example:

Social engineering phone call to force an employee to perform an action in SalesForce. Initial Access - T1566.004 (Spearphishing: Voice / vishing)

Execution: A victim is installing a fake Data Loader. Execution - T1204 (User Execution)

Collection:

a. Use of valid accounts- UNC6040 may directly request user credentials and multifactor authentication (MFA) codes and what we wrote above.
b. Stealing application access token
    - Authorization: The victim is persuaded to approve a malicious connected app, which is often a modified version of the Data Loader that is not authorized by Salesforce . The attacker guides the victim to enter a "connection code," which links the attacker-controlled Data Loader to the victim's environment
    - Capabilities Granted: This step inadvertently grants UNC6040 significant capabilities to access, query, and exfiltrate sensitive information directly from the compromised Salesforce customer environments.

c. Automated data collection and use of proxy/vpn/Tor-

- Evolving Tactics: While UNC6040 initially relied on the Salesforce Dataloader application, they have since evolved their tactics, techniques, and procedures (TTPs) to use custom applications, typically Python scripts, that perform similar functions. They have also been observed configuring their malicious application with misleading names like "My Ticket Portal," aligning with their IT support social engineering pretext.

d. Exfiltration-copy confidential data from cloud storage\internal systems. Technique- exfiltration to Cloud Storage. Once access is obtained, the threat cluster moves quickly to steal data

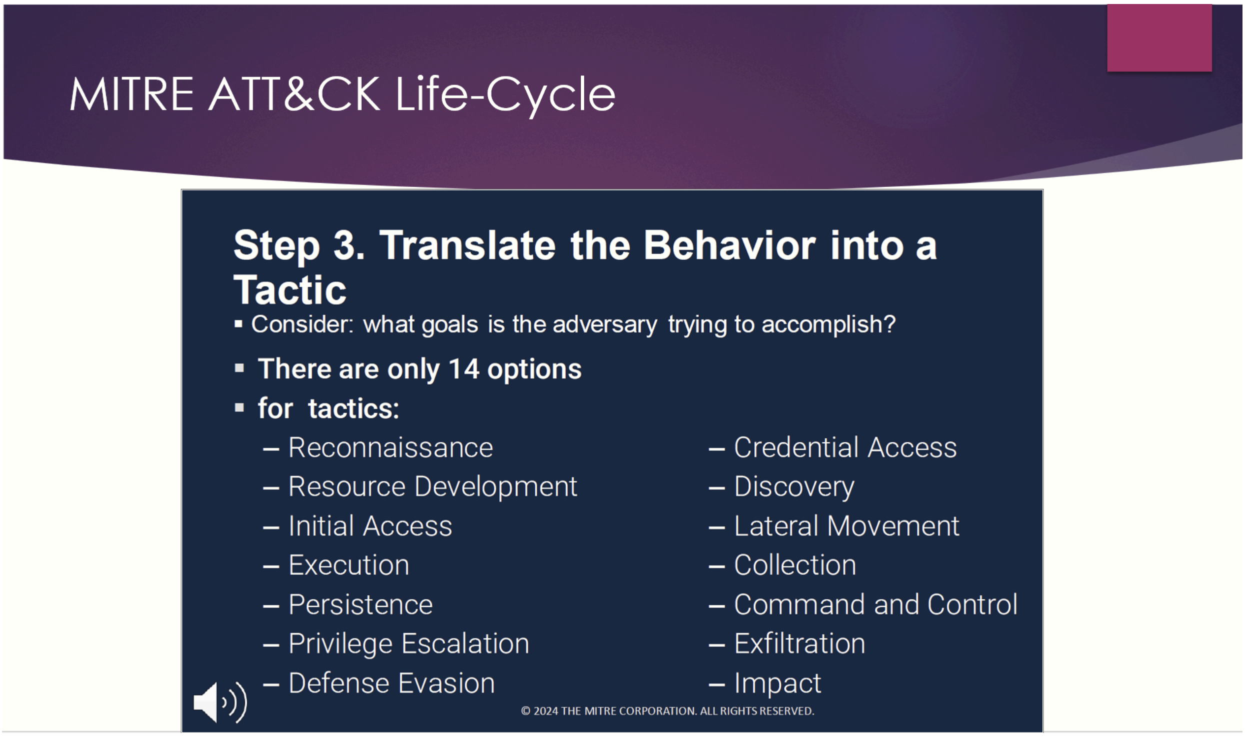
- *Immediate Exfiltration:* Upon obtaining access, UNC6040 has been observed immediately exfiltrating data from the victim's Salesforce environment using the Data Loader application or similar custom tools
- Using Infrastructure: The data collection is automated and performed through TOR IPs . UNC6040 primarily uses Mullvad VPN IP addresses to access and perform data exfiltration .
- Volume: Threat actors have demonstrated varied proficiency; in one instance, an actor could only retrieve about 10% of the data before access was revoked . In other cases, actors made initial small test queries and, once sufficient information was gathered, rapidly increased the exfiltration volume to extract entire tables.
- Lateral Movement: Following initial data theft, UNC6040 has been observed leveraging end-user credentials obtained through vishing or credential harvesting to move laterally through victim networks, exfiltrating data from other cloud platforms like Okta and Microsoft 365 .

<u>Credential Access: </u>harvest credentials from phishing sites. technique- multi-Factor Authentication Interception

<u>Persistence: </u>reuse valid credentials\ create new accounts for future access.technique- account Manipulation

Impact: threaten\ sell stolen data for financial gain -data extortion.
Technique-Data Encrypted for Impact / Data Leak

From the presentation:

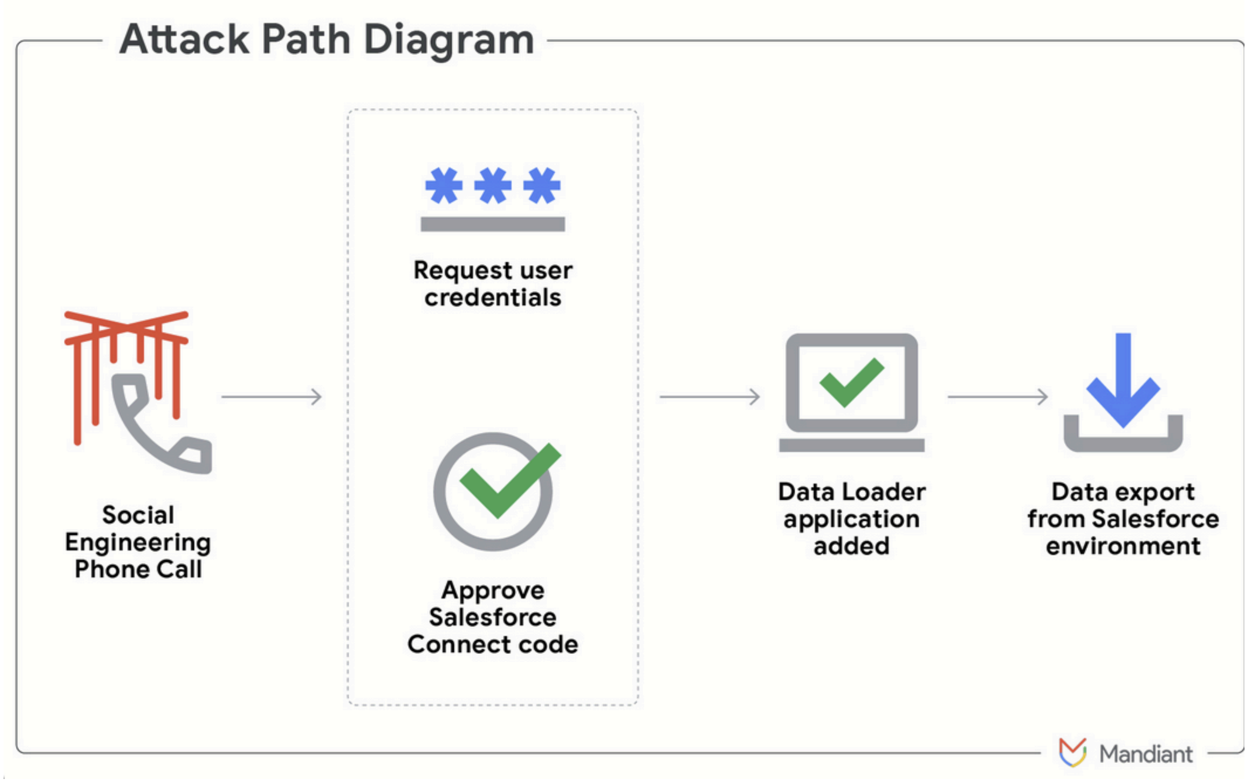


MITRE ATT&CK Life-Cycle

Step 3. Translate the Behavior into a Tactic

- Consider: what goals is the adversary trying to accomplish?
- **There are only 14 options**
- **for tactics:**
  - Reconnaissance
  - Resource Development
  - Initial Access
  - Execution
  - Persistence
  - Privilege Escalation
  - Defense Evasion
  - Credential Access
  - Discovery
  - Lateral Movement
  - Collection
  - Command and Control
  - Exfiltration
  - Impact

From the report:


Attack Path Diagram
Social Engineering Phone Call
Request user credentials
Approve Salesforce Connect code
Data Loader application added
Data export from Salesforce environment
Mandiant