Credential Theft

Incident Response Playbook
Suitable for all (private and public) organizations
Developed by: Olumuyiwa Olufunmilola Agunbiade

Credential Theft - Incident Response Playbook Template

Version history

Version	Update Date	Updated By	Reason for Update
1.0	9/23/2023	Olumuyiwa Agunbiade	Initial Draft

Purpose

To guide <ORGANIZATION> in responding to a credential theft incident.

How to Use This Playbook

The steps in this playbook should be followed sequentially where appropriate. With many steps in the Containment, Eradication, and Recovery steps, some overlap may occur and is expected.

Preparation

Note: Preparation steps should primarily be completed prior to an event or incident.

1. Determine the members of the Cybersecurity Incident Response Team (CSIRT).
    a. The core CSIRT members should be comprised of individuals responsible for cybersecurity only.
        i. This may include some members of Information Technology roles, depending on the organization size.
        ii. The limited size of the core CSIRT is to assist with confidentiality and efficiency.
        iii. The core CSIRT may be activated often to investigate security events that may or may not result in an incident.
    b. Assign roles and responsibilities to each member.
2. Determine extended CSIRT members.
    a. This will often be Legal, Compliance, Public Relations, and Executive Leadership.
3. Define escalation paths.
    a. Incidents may start as events, or as a lower impact/severity and then increase as more information is gathered. Establishing an escalation path is critical to success.

4. Ensure logging levels for account login system components (i.e. Active Directory, VPN, Remote Access, etc.) are set to appropriate levels.
    a. 90 days should be the minimum.
5. Ensure logging for account login system components are stored in secure locations, preferably on a secondary system such as a SIEM.

Identification

1. Use the evidence that resulted in notification of compromise to determine next steps based on method of compromise.**(Some steps may be irrelevant based on the method of compromise.)**
    a. Example of evidence: an email from an external client saying they received a phishing email or malware, abnormal login behavior or locations, actions performed by a user account that can't be accounted for by the user, etc.
    b. Method of compromise examples: credential harvesting phish, credential scraping from local systems, brute forced password, etc.
2. Determine initial method of account compromise.
    a. Interview impacted user to gather details on potential points of compromise.
        i. Example questions:
            1. Did you receive a suspicious email?
            2. Did you enter your email credentials after clicking a link, or on a website that seemed to not accept them?
            3. Have you downloaded any new software?
            4. Have you received any documents via email that you weren't expecting?
            5. Have no noticed abnormal actions on your workstation?
    b. Search for phishing emails.
        i. Phishing emails are the most common method for credential theft.
    c. Search for emails with links to credential harvesting sites.
    d. Search the user's web history to determine if any potentially malicious sites were visited.
    e. Search for potential malware on the user's workstation.
        i. Credential harvesters such as Mimikatz.
        ii. Keystroke recording software.
        iii. Clipboard scraping malware.
3. Once method of initial compromise is determined, use the Indicators of Compromise (IoCs) gathered to search the environment for other victims.
    a. Potential query inputs for email system: Email subject name, document name, document hash, URL from email, etc.
    b. Potential query inputs for SIEM or log searches: IP addresses, URLs, workstation names, etc.
4. Review logs in account login systems searching for anomalies.
    a. Login activity from unusual locations, systems, or browser fingerprints.
    b. Note all systems accessed by the attacker if possible.
5. Assess victim accounts to determine if sensitive information may be contained in them, or if they have access to sensitive information on centralized storage such as fileservers.
    a. This may need to be extended to other sources these users and/or accounts have access to such as OneDrive, Google Drive, SharePoint, shared mailboxes, fileservers, etc.
    b. If sensitive information is a possibility, consult legal counsel for next steps.
6. Use the information gathered in Step 4b to determine what sensitive information could've been accessed by the attacker.
    a. If logs are unavailable, assume all accessible data was accessed by the attacker.

Containment

1. Reset all passwords associated with all identified victims.
    a. Begin with the known compromised account passwords, but all accounts associated with the user should have their passwords reset or disabled.
2. Enable Multi-Factor authentication anywhere possible for the impacted user account.
3. Disable user account's ability to login remotely.
4. Revoke authentication tokens for all identified victim accounts.
    a. This should cover the email system and any other accounts that are associated with the impacted users.
5. If an external organization is identified during the investigation, notify the organization of any compromises or concerns.
    a. Work with legal counsel to determine this process.
    b. This will help prevent the organization's users from being targeted again from the same compromised source.
6. If an external organization is identified during the investigation, block their related domains from sending email to your organization.
7. If malware is discovered during the investigation:
    a. Preserve a sample of the malware.
    b. Analyze the malware with any tools available.
        i. Gather file hash using PowerShell "Get-Filehash" cmdlet.
        ii. Submit hash to community sourcesVirusTotal, Hybrid-Analysis, etc.
            1. If community sources have seen the hash, note the malware characteristics.
    c. Isolate infected systems, do not power them off unless absolutely necessary.
        i. Preserve the system(s) for further forensic investigation including log review, MFT analysis, deep malware scans, etc.
8. Block all associated IoCs in email system, firewall, and other security components such as endpoint protection systems.
    a. URLs, domains, message-ID, etc. in spam filters, email based antimalware, etc.
    b. File hashes, malware identified, IP addresses identified, etc.

Eradication

1. Preserve artifacts, systems, and relevant backups according to the sensitivity and scale of the incident. These may be important for future forensics.
    a. If rebuilding or replacing physical systems, preserve physical hard disks, solid state drives, or forensically sound images of those storage drives.
    b. If rebuilding or replacing virtual machines, preserve a copy, full (independent) snapshot, or a backup of the system.
2. Preserve any volatile data that may have been collected during the identification and containment phases.
    a. This may include log files, backups, malware samples, memory images, etc.
3. Once all relevant data, equipment, and/or systems have been preserved,replace, or rebuild systems accordingly.

Recovery

1. Restore impacted systems from a clean backup, taken prior to infection if these backups are available.

2. For systems not restorable from backup, rebuild the machines from a known good image or from bare metal.
3. Remediate any vulnerabilities and gaps identified during the investigation.
4. Reset passwords for all impacted accounts and/or create replacement accounts and leave the impacted accounts disabled permanently.
5. Continue to monitor for malicious activity related to this incident for an extended period.
    a. Alerts should be configured to aid in quick detection and response.

Lessons Learned

1. Conduct a meeting after the incident to discuss the following:
    a. What things went well during the investigation?
    b. What things did not go well during the investigation?
    c. What vulnerabilities or gaps in the organization's security status were identified?
        i. How will these be remediated?
    d. What further steps or actions would have been helpful in preventing the incident?
    e. Do modifications need to be made to any of the following:
        i. Authentication practices?
            1. Multi-Factor Authentication
            2. Password complexity and use
        ii. Network segmentation
        iii. Firewall configuration
        iv. Application security
        v. Operating System and/or Application patching procedures
        vi. Employee, IT, or CSIRT training
2. Create and distribute an incident report to relevant parties.
    a. A primary, and more technical, report should be completed for the CSIRT.
    b. An executive summary should be completed and presented to the management team.

Question & Answer?