INCIDENT RESPONSE PLAYBOOKS

Business Email Compromise

Purpose

To guide <ORGANIZATION> in responding to a Business Email Compromise 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 if applicable (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.
        i. Summary of roles and responsibilities for avg CSIRT team
2. Determine extended CSIRT members.
    a. This will often be Legal, Compliance, Public Relations, and Executive Leadership.
    b. Summary of roles and responsibilities for extended CSIRT team
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.
    b. Give example of escalation path – including thresholds for escalation
4. Ensure logging levels for email system components are set to appropriate levels.
    a. 90 days should be the minimum.
    b. expand on what logging levels for email system components are, and how to check the current minimum and adjust accordingly if needed
    c. Show how on Google and Outlook
5. Ensure logging for email system components are stored in secure locations, preferably on a secondary system such as a SIEM.
    a. Define SIEM
    b. Give examples of good SIEM solutions

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, email rules that were not created by the user, a fraudulent funds transfer, etc.
    b. Method of compromise examples: credential harvesting phish, attached malware, 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?
    b. Search for phishing emails.
        i. Expand on finding phishing emails
    c. Search for emails with links to credential harvesting sites.
        i. Examples of credential harvesting sites and/or how to identify
    d. Search for potential malware on the user's workstation.
        i. Credential harvesters such as Mimikatz.
            1. How to find on the workstation
            2. Elaborate on what a credential harvester is
        ii. Keystroke recording software.
            1. How to find on the workstation
            2. Elaborate on what a keystroke rec. software
        iii. Clipboard scraping malware.
            1. How to find on the workstation
            2. Elaborate on what clipboard scraping malware is
3. Once method of initial compromise is determined, use the Indicators of Compromise (IoCs) gathered to search the environment for other victims.
    a. Elaborate on where the user should search, and what tools to use
    b. Potential query inputs: Email subject name, document name, document hash, URL from email, etc.
4. Review logs in email system searching for anomalies.
    a. Login activity from unusual locations, systems, or browser fingerprints.
    b. Compare any login anomalies to other logins with similar characteristics, such as:
        i. Originating IP address – elaborate/explain how to find + screenshots
        ii. Concurrent login – elaborate/explain how to find + screenshots
        iii. Browser fingerprint – elaborate/explain how to find + screenshots
5. Assess victim email accounts to determine if sensitive information may be contained in them.
    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.
        i. Give examples of sensitive info
6. Search impacted systems for newly created users.
    a. Ensure that all recently created users are accounted for.

Containment

1. Reset all passwords associated with all identified victims.
    a. Begin with email account passwords, but all accounts associated with the user should have their passwords reset or disabled.
2. Revoke authentication tokens for all identified victim accounts.
    a. Define authentication tokens + how to revoke them

    b. This should cover the email system and any other accounts that are associated with the impacted users.
3. 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.
4. If an external organization is identified during the investigation, block their related domains from sending email to your organization.
5. If malware is discovered during the investigation:
    a. Preserve a sample of the malware.
        i. Why you should do so
        ii. How to do so safely
    b. Analyze the malware with any tools available.
        i. Does analyzing the malware involve more than gathering the file hash? If so please explain more.
        ii. Gather file hash using PowerShell "Get-Filehash" cmdlet.
        iii. Submit hash to community sources VirusTotal, Hybrid-Analysis, etc.
            1. If community sources have seen the hash, note the malware characteristics.
            2. Depending on results – initiation of the malware outbreak playbook may be required.
    c. Isolate infected systems, do not power them off unless absolutely necessary.
        i. Describe how to isolate systems
        ii. Preserve the system(s) for further forensic investigation including log review, MFT analysis, deep malware scans, etc.
            1. Describe how to preserve the system,
            2. Give examples of the best deep malware scanners
            3. Define MFT analysis
6. Block all associated IoCs in email system components.
    a. URLs, domains, message-ID, etc. in spam filters, email based antimalware, etc.
7. Block all associated IoCs in endpoint protection systems.
    a. What is an endpoint protection system
    b. File hashes, malware 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. Retain copies of malicious emails and malware.
        i. Store in a safe location, password protected.
        ii. What makes a safe location
    b. If rebuilding or replacing physical systems, preserve physical hard disks, solid state drives, or forensically sound images of those storage drives.
    c. 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. What makes data volatile

    b. 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.
    a. Expand on how to replace or rebuild

Recovery

1. Remediate any vulnerabilities and gaps identified during the investigation.
2. Reset passwords for all impacted accounts and/or create replacement accounts and leave the impacted accounts disabled permanently.
    a. This may have been completed in a previous step but should be reviewed to ensure that all impacted accounts have been handled correctly.
3. 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.
        i. How do you set up alerts
        ii. Examples: Anomalous behavior such as login activity from unusual locations.
4. If financial loss was incurred, consult cybersecurity insurance.

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. Application security
        ii. Operating System and/or Application patching procedures
        iii. Employee, IT, or CSIRT training
        iv. Email filtering policies
        v. Multifactor Authentication
        vi. Email retention policies
        vii. Sensitive information policies and procedures related to email
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.

Credential Theft

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 sources VirusTotal, 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.

Lost or Stolen Device

Purpose

To guide <ORGANIZATION> in responding to a lost or stolen device 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. Determine controls for lost or stolen devices.
    a. Remote wipe capabilities.
    b. At-rest encryption.
    c. Multi-Factor Authentication.

Identification

1. Identify the nature of the device that has been lost or stolen.
    a. Laptop?
    b. Phone?
    c. Tablet?
    d. Other device such as desktop, server, other equipment, etc.
2. Assess the criticality of data or accounts that may be present on the device.
3. Interview the user to understand the conditions around the lost or stolen device.
    a. Was it misplaced?
    b. Can you confirm that it was stolen?
    c. Was the device logged in and active to any accounts?
4. Contact local authorities to report the loss.

a. Clear this process with legal counsel first.

Containment and Eradication

1. Disable or reset the password for any accounts that may be accessed via the lost or stolen device.
2. Perform remote wipe capabilities to eradicate any sensitive data on the lost or stolen device.
3. If the device is a laptop or other computer:
    a. Disable any active directory accounts for the device.
    b. Create alerts for any time the device contacts the network.
    c. Disable any remote access associated with the device.
        i. i.e. VPN accounts and certificates, Microsoft InTune, Exchange ActiveSync, JAMF, etc.
    d. Remind user to disable or reset the password for any personal accounts in use on the device.
4. If the device is a phone, tablet, or other mobile device:
    a. Disable active directory accounts for the device if applicable.
    b. Disable any remote access associated with the device.
        i. i.e. VPN accounts and certificates, Microsoft InTune, Exchange ActiveSync, JAMF, etc.
    c. Create alerts for any time the device attempts to check-in or contact the network.
    d. Contact the cellular provider to notify them that the device has been lost or stolen and any associated hardware addresses should be blocked from access.
    e. Remind user to disable or reset the password for any personal accounts in use on the device.

Recovery

1. Restore user work functionality with a trusted device.
2. Create alerts for any abnormal activity from the user accounts involved.

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. Remote management capabilities
        ii. Application security
        iii. Employee, IT, or CSIRT training
        iv. Encryption capabilities
        v. Access rights to sensitive information
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.

Malware Outbreak

Purpose

To guide <ORGANIZATION> in responding to a malware outbreak 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. If the playbook is being accessed during an event or incident you may proceed to Preparation Step 4b.

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. Evaluate and secure critical system backups.
    a. Backups should be secured prior to any incident.
    b. During the initial stages of any incident, evaluate and confirm that backups are secure and not impacted by the incident.

Identification

1. Isolate infected systems ASAP.
    a. DO NOT power off machines, as forensic artifacts may be lost.
    b. Preserve the system(s) for further forensic investigation including log review, MFT analysis, deep malware scans, etc.
        i. These steps should be performed during the Identification phase to guide the investigation.
2. Investigate malware to determine if it's running under a user context.
    a. If so, disable this account (or accounts if multiple are in use) until the investigation is complete.
3. Analyze the malware to determine characteristics that may be used to contain the outbreak.
    a. If available, use a sandboxed malware analysis system to perform analysis.

        i. **Note:** Network connectivity should not be present for this sandbox system except in very rare circumstances. Network activity from malware may be used to alert an attacker of your investigation.
        ii. Observe any attempts at network connectivity, note these as Indicators of Compromise (IoCs)
        iii. Observe any files created or modified by the malware, note these as IoCs.
        iv. Note where the malware was located on the infected system, note this as an IoC.
        v. Preserve a copy of the malware file(s) in a password protected zip file.
    b. Use the PowerShell "Get-FileHash" cmdlet to get the SHA-256 hash value of the malware file(s).
        i. This hash may also be used to search for community information regarding this malware (i.e. VirusTotal, Hybrid-Analysis, CISCO Talos, etc.)
        ii. Additional hash values (SHA1, MD5, etc.) may be gathered to better suit your security tools.
        iii. Note these hash values as IoCs.
    c. Use all IoCs discovered to search any available tools in the environment to locate additional infected hosts.
4. Use all information and IoCs available to determine if the malware is associated with further attacks.
    a. i.e. Emotet, Trickbot, and Qakbot are often involved in Ryuk ransomware attacks.
    b. If further attacks are associated, gather all additional information available on these attacks to further the investigation.
5. Use all information and IoCs available to search for the initial point of entry.
    a. Determine the first appearance of the malware.
    b. Determine the user first impacted by the malware.
    c. Investigate all available log files to determine the initial date and point of infection.
    d. Analyze all possible vectors for infection.
        i. Focus on known delivery methods discovered during malware analysis (email, PDF, website, packaged software, etc.).

Containment

1. Use the information about the initial point of entry gathered in the previous phase to close any possible gaps.
    a. Examples: Firewall configuration changes, email blocking rules, user education, etc.
2. Once the IoCs discovered in the Identification phase have been used to find any additional hosts that may be infected, isolate these devices as well.
3. Add IoCs (such as hash value) to endpoint protection.
    a. Set to block and alert upon detection.
4. Submit hash value to community sources to aid in future detection.
    a. **NOTE:** Clear this process with legal/compliance representatives during each incident, as each malware situation will be different.
5. If additional further attacks were noted as associated with the malware, use IoCs and threat-intel to apply additional controls to prevent the attack from escalating.
6. Implement any temporary network rules, procedures and segmentation required to contain the malware.
7. If additional accounts have been discovered to be involved or compromised, disable those accounts.

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. Network segmentation
        ii. Firewall configuration
        iii. Application security
        iv. Operating System and/or Application patching procedures
        v. 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.

Ransomware

Purpose

To guide <ORGANIZATION> in responding to a ransomware 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. If the playbook is being accessed during an event or incident you may proceed to Preparation Step 4b.

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. Evaluate and secure critical system backups.
    a. Backups should be secured prior to any incident.
    b. During the initial stages of any incident, evaluate and confirm that backups are secure and not impacted by the incident.

Identification

1. Isolate infected systems ASAP.
    a. DO NOT power off machines, as forensic artifacts may be lost.
    b. Preserve the system(s) for further forensic investigation including log review, MFT analysis, deep malware scans, etc.
        i. These steps should be performed during the Identification phase to guide the investigation.
2. Investigate malware to determine if it's running under a user context.
    a. If so, disable this account (or accounts if multiple are in use) until the investigation is complete.
3. Analyze the malware to determine characteristics that may be used to contain the outbreak.
    a. If available, use a sandboxed malware analysis system to perform analysis.

        i. **Note:** Network connectivity should not be present for this sandbox system except in very rare circumstances. Network activity from malware may be used to alert an attacker of your investigation.
        ii. Observe any attempts at network connectivity, note these as Indicators of Compromise (IoCs)
        iii. Observe any files created or modified by the malware, note these as IoCs.
        iv. Note where the malware was located on the infected system, note this as an IoC.
        v. Preserve a copy of the malware file(s) in a password protected zip file.
    b. Use the PowerShell "Get-FileHash" cmdlet to get the SHA-256 hash value of the malware file(s).
        i. This hash may also be used to search for community information regarding this malware (i.e. VirusTotal, Hybrid-Analysis, CISCO Talos, etc.)
        ii. Additional hash values (SHA1, MD5, etc.) may be gathered to better suit your security tools.
        iii. Note these hash values as IoCs.
    c. Use all IoCs discovered to search any available tools in the environment to locate additional infected hosts.
4. Use all information and IoCs available to search for the initial point of entry.
    a. Determine the first appearance of the malware.
    b. Determine the user first impacted by the malware.
    c. Investigate all available log files to determine the initial date and point of infection.
    d. Analyze all possible vectors for infection.
        i. Focus on known delivery methods discovered during malware analysis (email, PDF, website, packaged software, etc.).
5. Once the ransomware variant is identified, perform research to determine Tactics, Techniques, and Procedures (TTPs) associated with this variant and/or threat-actor.
    a. Determine if data exfiltration and extortion is common.
    b. Determine attacker toolkit if possible.

Containment

1. Use the information about the initial point of entry gathered in the previous phase to close any possible gaps.
    a. Examples: Firewall configuration changes, email blocking rules, user education, etc.
2. Once the IoCs discovered in the Identification phase have been used to find any additional hosts that may be infected, isolate these devices as well.
3. Add IoCs (such as hash value) to endpoint protection.
    a. Set to block and alert upon detection.
4. Submit hash value to community sources to aid in future detection.
    a. **NOTE:** Clear this process with legal/compliance representatives during each incident, as each malware situation will be different.
5. Implement any temporary network rules, procedures and segmentation required to contain the malware.
6. If additional accounts have been discovered to be involved or compromised, disable those accounts.

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.
6. If data-exfiltration and extortion were determined to be part of this attack, work with legal counsel to determine next steps.

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. Network segmentation
        ii. Firewall configuration
        iii. Application security
        iv. Operating System and/or Application patching procedures
        v. 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.

Web Application Compromise

Purpose

To guide <ORGANIZATION> in responding to a web application compromise incident. This playbook may also be used for a website defacement 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. Document third-party web-hosting contacts.
5. Ensure logging levels for account login system components are set to appropriate levels.
    a. 90 days should be the minimum.
6. Ensure logging for account login system components are stored in secure locations, preferably on a secondary system such as a SIEM.
7. Ensure that web application backups are functioning as expected.

Identification

1. If the web application is hosted on another service (GoDaddy, HostGator, Ionos, local hosting company, etc.) contact the hosting service to report the issue.
    a. Inquire as to any recent security issues in their environment.
    b. Inquire about any potential logs that they may possess.
        i. Obtain these logs and preserve them ASAP.
2. 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: abnormal behavior in the web application, notification of compromise from an outside source, client report of anomalous or malicious behavior related to the web application, etc.

    b. Method of compromise examples: exploited vulnerability in web application, credential harvesting phish, credential scraping from local systems, brute forced password, etc.
3. Determine initial method of account compromise. This will be limited to those with web application management/administrative access.
    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.
4. 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.
5. 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.
6. 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.
7. 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.
8. If account compromise has been ruled out, proceed to investigate potential web application vulnerabilities that may have been exploited.
    a. Perform a security scan.
    b. Review vendor notifications of security issues.
    c. Review community sourced threat-intelligence related to the components in your web application.

Containment

1. If management or administrative account compromise has been determined:
    a. Reset all passwords associated with management and administration of the web application.
        i. Begin with the known compromised account passwords (if determined).

    b. Enable Multi-Factor authentication anywhere possible for the impacted account(s).
    c. Disable or reset alternative authentication methods such as certificates.
    d. Revoke authentication tokens for all management/administrative account(s).
2. 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.
3. 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 sources VirusTotal, 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.
4. 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.
5. Preserve a copy of any existing web application code that may be compromised and/or altered maliciously.

Eradication

1. Compare current web application code to a known-good copy to determine if any malicious additions have been removed.
2. If systems were determined to be compromised with malware or by other means:
    a. Preserve artifacts, systems, and relevant backups according to the sensitivity and scale of the incident. These may be important for future forensics.
        i. If rebuilding or replacing physical systems, preserve physical hard disks, solid state drives, or forensically sound images of those storage drives.
        ii. If rebuilding or replacing virtual machines, preserve a copy, full (independent) snapshot, or a backup of the system.
3. Preserve any volatile data that may have been collected during the identification and containment phases.
    a. This may include log files, code samples, backups, malware samples, memory images, etc.
4. Review and monitor logs to ensure that the compromise has been entirely contained.
5. Once all relevant data, web application code samples, or other potential items of evidence have been preserved, proceed to Recovery.

Recovery

1. Replace potentially compromised web application code with a known-good copy.
    a. This may be completed by removing code anomalies or from restoring a known-good copy.
2. Review current web application code to ensure that all code anomalies have been removed.

    a. This should be a new review, preferably by a different individual than the one who performed the review in Eradication step 1.
3. Restore web application functionality.
4. Restore impacted systems from a clean backup, taken prior to infection if these backups are available.
5. For systems not restorable from backup, rebuild the machines from a known good image or from bare metal.
6. Remediate any vulnerabilities and gaps identified during the investigation.
7. Reset passwords for all impacted accounts and/or create replacement accounts and leave the impacted accounts disabled permanently.
8. 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. Change control practices
        ii. Code review practices
        iii. Authentication practices
            1. Multi-Factor Authentication
            2. Password complexity and use
            3. Privileged account access
        iv. Network segmentation
        v. Firewall configuration
        vi. Application security
        vii. Operating System and/or Application patching procedures
        viii. 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.