Playbook: Website Defacement

Investigate, remediate (contain, eradicate), and communicate in parallel!

Assign steps to individuals or teams to work concurrently, when possible; this playbook is not purely sequential. Use your best judgment.

Investigate

1. Immediately take the defaced server offline for further investigation
    - This is especially important if the defacement is insulting or triggering in any way. Remove this from the public eye as quickly as possible to avoid harm as well as to mitigate business impact.
    - The defacement message may also contain false information that could mislead users or put them at risk.
    - Taking the server offline will allow a deeper investigation of the defacement. This may be necessary as the hacker may have dove depper into the organization accessing application servers, databases, etc.
2. Determine the system's source of vulnerability that was used by the attacker. Common exploits include:
    - SQL injection attakcs
        - This kind of attack occurs when an attacker interferes with an application's queries to the database. Therefore, this can lead to unauthorized access to private or sensitive data. Read more about SQL injection attacks here (https://www.acunetix.com/websitesecurity/sql-injection/)
    - Remote File Inclusion (RFI) attacks
        - This kind of attack exploits an application's referencing function to upload malware from a remote URL. Read more about RFI attacks here (https://www.acunetix.com/blog/articles/remote-file-inclusion-rfi/)
    - webshells
        - More about web shells and website defacement here (https://www.wordfence.com/blog/2017/06/wso-shell/)
    - poor web application design
        - javascript hacks
        - PHP/ASP hacks
        - Here's more on hacking with javascript (https://itnext.io/how-companies-are-hacked-via-malicious-javascript-code-12aa82560bdc)
    - other methods of detection include:
        - Checking the server logs
            - look through the web page's access log and error log for any suspicious or unfamiliar activity
            - of course, it is also a good idea to check the IDS or IPS firewall logs, if available
        - Checking files with static content
        - Scanning databases for malicious content
        - Checking links present in the page
3. Collect any clues as to who the hacker is or what organization they are working for. Consider the following questions:
    - What did the defacement portray? Did it include an obvious message?

    - Did the defacement seem harmless or intentional? Could the hacker be a kid messing around or a professional group working with a motive?
    - Does it seem like your organization was targeted? Who may want to target your organization?
    - What did the hacker hope to accomplish?
    - Consult here (https://www.geeksforgeeks.org/types-of-hackers/) to learn more about the types of hackers that may have attacked your webpage.
4. Collect other important information from the page that has been defaced such as:
    - a screenshot of the defacement
    - the domain and IP address of the page
    - details of the web server
    - page's source code
        - analyze this carefully to identify the problem and ensure that it is on a server belonging to the company
    - name or any information on the attacker
5. There are also tools available to aid in both detection and log analysis. A few are listed below:
    - Weblog Expert
    - Sawmill
    - Deep Log Analyzer

`TODO: Expand investigation steps, including key questions and strategies, for website defacement.`

Remediate

- **Plan remediation events** where these steps are launched together (or in coordinated fashion), with appropriate teams ready to respond to any disruption.
- **Consider the timing and tradeoffs** of remediation actions: your response has consequences.

Contain

`TODO: Customize containment steps, tactical and strategic, for website defacement.`

`TODO: Specify tools and procedures for each step, below.`

1. Backup all data stored on the web server for forensic purposes.
2. As previously mentioned, make sure to take the defaced page's server down temporarily while investigation occurs.
    - You should have an error page prepared for this situation that informs user and/or employees that maintenance is undereway and the page they sought will return shortly. You may even wish to have a backup website prepared where you may publish content while investigation and remediation are underway and have your temporary error page redirect users to this backup site.
    - Check your network architecture map. If the breach is another system on the network, take that down and investigate it.
3. Once the source of the attack has been determined, apply the necessarily steps to ensure this will not happen again. This may include modifying code or editing access rights.

- Reference the "Investigate" section for common sources of vulnerability.
- If this is outside of your domain, simply ensure that you have given the appropriate personnel all the information on the attack that you have and allow experts to do their job.

Recover

`TODO: Customize recovery steps for defacement`

`TODO: Specify tools and procedures for each step, below`

1. Remove the hacker's message and replace with original, legitimate content. If data was lost in the attack, reference backups and restore the original page as much as possible.
    - Check backups for indicators of compromise
    - Consider partial recovery and backup integrity testing
2. Consider asking users to change their login credentials if the web server has user authentication.
3. After implementing risk avoidance measures (as recommended below), restore your server showing the original page content.
4. If necessary and/or applicable, prepare an apology/explanation of the attack that occurred for users or anyone who witnessed the defacement. Ensure that is it clear that the defacement content does not reflect your organization in any way.

Risk Avoidance

`TODO: Communicate with other employees to ensure that everyone understands and contributes to the following steps, where applicable`

1. Use as few plug-ins as necessary. Hackers target websites that are vulnerable and have many sources of entry. You can limit these sources of entry by only using what you need and removing any unused or old plug ins and software. It is also important to update these as soon as possible.
2. Closely monitor and mandate access to administrative content. Only allow individuals access to what they need access to. This will reduce the chance of human error leading to cyber attacks. There are more DIY methods of prevention mentioned in this article (https://cirt.gy/index.php/node/116) (steps 6-12) and in resource #4 at the end of this playbook.
3. Regularly check for malware on your site by scanning the source code. Look for scripts, iframes, or URLs that look unfamiliar and make sure to also scan URLs that do look familiar.
4. There are many highly reputable automated website scanners that will not cost any of your time and will thoroughly scan your site for vulnerabilities regularly. Here is a link to popular scanners (https://resources.infosecinstitute.com/14-popular-web-application-vulnerability-scanners/#gref).
5. Defend against common points of exploitation such as SQL injections and XSS attacks. This article (https://www.banffcyber.com/knowledge-base/articles/best-practices-address-issue-web-defacement/) includes best practices to defend these attacks.
6. Install defacement detection programs so that if an attack were to occurr again, you would be prepared and respond quickly. Here is an article (https://www.techradar.com/news/best-website-defacement-monitoring-service) that summarizes some of 2020's best monitoring services.

7. Discuss with your employees the importance of keeping administrative access limited and confidential and inform them of these steps to avoid incidents including regular cybersecurity awareness training.

Reference: Remediation Resources

`TODO: Specify financial, personnel, and logistical resources to accomplish remediation`

Communicate

`TODO: Customize communication steps for defacement`

`TODO: Specify tools and procedures (including who must be involved) for each step, below, or refer to overall plan`

1. Escalate incident and communicate with leadership per procedure
2. Document incident per procedure (and report if applicable)
3. Communicate with internal and external legal counsel per procedure, including discussions of compliance, risk exposure, liability, law enforcement contact, *etc.*
4. Communicate with users (internal)
    1. Communicate incident response updates per procedure
    2. Communicate impact of incident **and** incident response actions (e.g., containment: "why is the file share down?")
    3. Communicate requirements: "what should users do and not do?"
5. Communicate with customers
    1. Focus particularly on those whose data was affected
    2. Generate required notifications based on applicable regulations (particularly those that may consider defacement a data breach or otherwise requires notifications) `TODO: Expand notification requirements and procedures for applicable regulations`
6. Contact insurance provider(s)
    1. Discuss what resources they can make available, what tools and vendors they support and will pay for, *etc.*
    2. Comply with reporting and claims requirements to protect eligibility
7. Consider notifying and involving law enforcement. TODO: Link the following bullets to actual resources for your organization
    1. Local law enforcement
    2. State or regional law enforcement
    3. Federal or national law enforcement
8. Communicate with security and IT vendors TODO: Link the following bullets to actual resources for your organization
    1. Notify and collaborate with managed providers per procedure
    2. Notify and collaborate with incident response consultants per procedure

Resources

Reference: User Actions for Suspected Defacement Attack

`TODO: Customize steps for users dealing with suspected defacement`

1. Stay calm, take a deep breath.
2. Disconnect your system from the network `TODO: include detailed steps with screenshots, a pre-installed tool or script to make this easy ("break in case of emergency"), consider hardware network cut-off switches`
3. Take pictures of the page you see using your smartphone showing the things you noticed: the defacement message and any other changes to the usual site.
4. Take notes about the problem(s) using the voice memo app on your smartphone or pen-and-paper. Every little bit helps! Document the following:
    1. What did you notice?
    2. When did it first occur, and how often since?
    3. What data do you typically access?
    4. Who else have you contacted about this incident, and what did you tell them?
5. Contact the help desk and be as helpful as possible.
6. Be patient: allow the IT personnel get it under control, you may be protecting others from harm! **Thank you.**

Reference: Help Desk Actions for Suspected Defacement Attack

`TODO: Customize steps for help desk personnel dealing with suspected defacement`

1. Stay calm, take a deep breath.
2. Open a ticket to document the incident, per procedure. `TODO: Customize template with key questions (see below) and follow-on workflow`
3. Use your best judgement on which steps to prioritize (i.e. if the defacement left harmful or triggerring content, prioritize taking down the server immediately).
4. Ask the user to take pictures of their screen using their smartphone showing the things they noticed.
5. Take notes about the problem(s) using the voice memo app on your smartphone or pen-and-paper. If this is a user report, ask detailed questions, including: 1. What did you notice?
    1. When did it first occur, and how often since?
    2. What data do you typically access?
    3. Who else have you contacted about this incident, and what did you tell them?
6. Ask follow-up questions as necessary. **You are an incident responder, we are counting on you.**
7. Get detailed contact information from the user (home, office, mobile), if applicable.
8. Record all information in the ticket, including hand-written and voice notes.
9. Quarantine affected users and systems. `TODO: Customize containment steps, automate as much as possible`
10. Contact the security team and stand by to participate in the response as directed: investigation, remediation, communication, and recovery.

Additional Information

1. A helpful and detailed paper (https://pdfs.semanticscholar.org/899e/2d629e06d920b9059edb21fcb52cdb33f783.pdf) on defacement detection
2. 10 tools for better website monitoring and security (https://geekflare.com/website-defacement-monitoring/)

3. 2019 Website Threat Research Report (https://sucuri.net/reports/2019-hacked-website-report/) with helpful statistics
4. Article (https://www.imperva.com/learn/application-security/website-defacement-attack/) including DIYs and Best practices to prevent website defacement