FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

18 August 2016

Alert Number

T-LD1004-TT

WE NEED YOUR HELP!

If you find any of these indicators on your networks, or have related information, please contact **FBI CYWATCH immediately**.

Email:

cywatch@ic.fbi.gov

Phone:

1-855-292-3937

**Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

In furtherance of public-private partnerships, the FBI routinely advises private industry of various cyber threat indicators observed during the course of our investigations. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber criminals.

This FLASH has been released **TLP: AMBER: The information in this product is only for members of their own organization and those with DIRECT NEED TO KNOW. This information is NOT to be forwarded on beyond NEED TO KNOW recipients.**

Targeting Activity Against State Board of Election Systems

Summary

The FBI received information of an additional IP address, 5.149.249.172, which was detected in the July 2016 compromise of a state's Board of Election Web site. Additionally, in August 2016 attempted intrusion activities into another state's Board of Election system identified the IP address, 185.104.9.39 used in the aforementioned compromise.

Technical Details

The following information was released by the MS-ISAC on 1 August 2016, which was derived through the course of the investigation.

In late June 2016, an unknown actor scanned a state's Board of Election website for vulnerabilities using Acunetix, and after identifying a Structured Query Language (SQL) injection (SQLi) vulnerability, used SQLmap to target the state website. The majority of the data exfiltration occurred in mid-July. There were 7 suspicious IPs and penetration testing tools Acunetix, SQLMap, and DirBuster used by the actor, detailed in the indicators section below.

Indicators associated with the Board of Elections intrusion:

- The use of Acunetix tool was confirmed when "GET /acunetix-wvs-test-for-some-inexistent-file - 443" and several requests with "wvstest=" appeared in the logs;

- The user agent for Acunetix was identified in the logs – "Mozilla/5.0+(Windows+NT+6.1;+WOW64)+AppleWebKit/537.21++(KHTML,+like+Gecko)+Chrome/41.0.2228.0+Safari/537.21";

- The use of SQLMap was confirmed after "GET /status.aspx DLIDNumber=1';DROP TABLE sqlmapoutput" appeared in the logs;

- The user agent for SQLMap is "Mozilla/5.0+(Macintosh;+U;+Intel+Mac+OS+X+10.7;+en-US;+rv:1.9.2.2)+Gecko/20100316+Firefox/3.6.2 200 0 0 421" (These are easily spoofed and not inclusive of all SQLMap activity);

- The user agent for the DirBuster program is "DirBuster-1.0-RC1+(http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project<http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project>)";

IP Addresses:

- 185.104.11.154
- 185.104.9.39
- 204.155.30.75
- 204.155.30.76
- 204.155.30.80
- 204.155.30.81
- 89.188.9.91
- 5.149.249.172 (new, per FBI)

Recommendations

The FBI is requesting that states contact their Board of Elections and determine if any similar activity to their logs, both inbound and outbound, has been detected. Attempts should not be made to touch or ping the IP addresses directly.

Recommended Steps for Precautions

The FBI recommends all states take the following precautions to their state Board of Election databases:

- Search logs for commands often passed during SQL injection: SELECT, INSERT, UNION, CREATE, DECLARE, CAST, EXEC, and DELETE, ‘, %27, --

- Search logs for privilege escalation attempts
  - Looking for references to “cmd.exe” and “xp_cmdshell” (IIS only)
  - Common to see these following SQL injection (logical next step)
  - Can limit search to entries with HTTP status code 200 (success)

- Search for signs of directory enumeration/traversal of the web server file system (used to identify the type of scripting language a web server supports)
    - *Looking for series of unsuccessful connections with strange URI strings, such as*:
        - GET /Login//..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5cetc/passwd
        - GET /images"OTA2NjAw%40
        - GET /Login//../../../../../../../../etc/passwd
        - GET /Login//../../../../../../../../windows/win.ini
            - Shortly after these requests you should see SQL injection in the logs
            - May also be "..\..\.."

The following recommendations were released by the MS-ISAC on 1 August 2016.

- Conduct vulnerability scans on local government and law enforcement websites and promptly remediate any vulnerabilities (or contact your hosting provider to do so on your behalf). Particular attention should be paid to SQLi vulnerabilities. Website hosting providers should also pay attention to vulnerabilities on other websites on the same server, which may provide a back-door into the local government's website.

- Ensure all software and applications, especially content management software, are fully patched.

- Create custom, general error messages for the web application to generate, as malicious cyber actors can gain valuable information, such as table and column names and data types, through default error messages generated by the database during a SQLi attack.

- Validate user input prior to forwarding it to the database. Only accept expected user input and limit input length. This can be done by implementing a whitelist for input validation, which involves defining exactly what input is authorized.

- Implement the principle of least privilege for database accounts. Administrator rights should never be assigned to application accounts and any given user should have access to only the bare minimum set of resources required to perform business tasks. Access should only be given to the specific tables an account requires to function properly.

- The database management system itself should have minimal privileges on the operating system, and since many of these systems run with root or system level access by default, it should be changed to more limited permissions.

- Isolate the web application from the SQL instructions. Place all SQL instructions required by the application in stored procedures on the database server. The use of user-created stored procedures and prepared statements (or parameterized queries) makes it nearly impossible for a user's input to modify SQL statements because they are compiled prior to adding the input. Also, have the application sanitize all user input to ensure the stored procedures are not susceptible to SQLi attacks.

- Use static queries. If dynamic queries are required, use prepared statements.

- Enable full logging on web servers and email servers to aid in forensic and legal responses if a breach does occur.

Information in this product is for official use only. No portion of this FLASH should be released to the media or the general public. Organizations should not attempt to connect to any of the IP addresses or domain names referenced in this FLASH. The indicators are being provided for network defense purposes only and any activity to these indicators or release of this material could adversely affect investigative activities.

Reporting Notice

The FBI encourages recipients who identify the use of tool(s) or techniques discussed in this document to report information to their local FBI Field Office or the FBI's 24/7 Cyber Watch (CyWatch). Field Office contacts can be identified at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at 855-292-3937 or by e-mail at CyWatch@ic.fbi.gov. When available, each report submitted should include: the date; time; location; type of activity; number of infected users; type of equipment used for the activity; name of the submitting company or organization; and a designated point of contact.