APT34 Web Shell Attack Targeting UAE Entities

ae CERT
فريق الاستجابة لطوارئ الحاسب الآلي
Computer Emergency Response Team

Security Advisory	ADV-19-08	**Criticality**	Critical	○○○●
Advisory Released On	4 April 2019			

Impact

Uploading a web shell on a victim's server may allow the attacker to remotely bypass security and gain access to the system.

Solution

Refer to the solution section.

Affected Platforms

- Web Servers.

Summary

As the leading trusted secure cyber coordination center in the region, aeCERT has researched and discovered a web shell attack targeting multiple UAE governmental entities. A web shell can allow an attacker to gain privileged access to a system and execute further attacking techniques on the affected server.

Threat Details

aeCERT has received reports from its intelligence sources indicating that APT34/OilRig has conducted a web shell based attack on multiple UAE government entities. A follow-up advisory containing a technical report of the attack will be provided on a later-date.

A web shell script can be uploaded to a web server allowing the attackers to gain remote administration of the machine. A web shell can be uploaded to servers either Internet-facing or internal to the network, afterwards the web shell can be utilized to pivot further towards internal hosts.

An attacker can use network scanning/reconnaissance tools to find vulnerabilities in the web server software or the web server itself to upload a web shell.

If the attacker successfully uploads the web shell, he can utilize it to leverage other attack methods in order to acquire administrative privileges and issue commands remotely. This grants the attacker the ability to modify, create, delete and launch files as well as granting him the ability to run more scripts, executables or shell commands.

The web shell script can be flexible as it can be written using any language that the target server is running. Web shells have been sighted running on the most common languages, such as ASP and PHP. As well as Python, Perl, Ruby, and Unix shell scripts.

Solution

In order to mitigate or detect the attack, we highly recommend the following:

Detection:

Web shells can be simple in nature which makes them hard to detect and anti-virus products can have a hard time detecting them but here are some suggestions that can assist you in detecting a web shell:

1- Files with unusual modification dates/timestamp.
2- Increased web traffic.
3- Look for files that include suspicious references to keywords such as cmd.exe.
4- Look for suspicious shell scripts such as ones that allow travelling between directories.

Mitigation:

1- Frequently update server to address most common vulnerabilities.
2- Apply proper and secure configuration when installing any server.
3- Utilize web application security such as firewall and frequently update virus signatures.
4- Apply a least-privileges policy on your web server.

Contact Us

aeCERT
P.O. Box 116688
Dubai, United Arab Emirates

Tel	(+971) 4 777 4003
Fax	(+971) 4 777 4100
Email	info[at]aeCERT.ae
Instagram	@TheUAETRA
Twitter	@TheUAETRA

For secure communications with aeCERT with regards to sensitive or vulnerability information please send your correspondences to aeCERT[at]aeCERT.ae