uila

Uila for Webshell Threat Detection

What is webshell?

As defined by CISA, a web shell is a script that can be uploaded to a web server to enable remote administration of the machine. Infected web servers can be either Internet-facing or internal to the network, where the web shell is used to pivot further to internal hosts. Once successfully uploaded, an attacker uses the web shell to leverage other exploitation techniques to escalate privileges and to issue commands remotely. These commands include the ability to add, delete, and execute files as well as the ability to run shell commands, further executables, or scripts.

Common Attack scenario

One of the common ways of delivering the webshell are techniques like SQL injection, Cross Site Scripting, Remote File Injection, Local File Include, etc, This includes the installation of a malicious file that will act as a webshell. Then the attacker develops an HTTP POST request directly to the webShell, with its malicious embedded commands to execute. And all of this will appear as if the attacker had local shell access to the web server.

Uila solution for Webshell Threat Detection

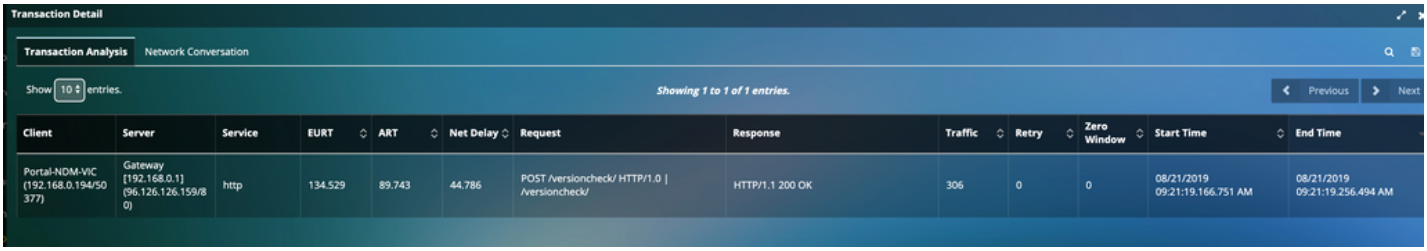
Uila can automatically identify via its built-in threat detection capability an attack from common webshells including:

- China Chopper: A malicious webshell that affects Windows and Linux servers. Known for its small size, Chopper can be employed as a Remote Access Tool (RAT) to perform the following file operations: upload, download, edit, copy, rename, delete, and modify timestamp.
- JSP webshell: This is used to maliciously manage an Apache Tomcat server. This webshell allows the attacker to have full control of the server by uploading, downloading, creating, editing and deleting files of the server. It can also open a proxy in the server and allow remote access to the server via a remote terminal.
- Jexbox webshell: A web shell from the JexBoss security tool was used to exploit servers through an unpatched JBoss vulnerability.
- WSO: Stands for “web shell by orb” and has the ability to masquerade as an error page containing a hidden login form.
- Many more...

Uila also identifies the SQL injection, Remote FIle Injection techniques. Few examples include:

- SQL generic sql update injection attempt - POST parameter
- SQL injection vulnerability in ProFTPD Server 1.3.1 through 1.3.2rc2 allows remote attackers to execute arbitrary SQL commands via a "%" (percent) character in the username, which introduces a "'" (single quote) character during variable substitution by mod_sql.
- SQL injection vulnerability in the WordPress Rencontre plugin.
- Multiple SQL injection vulnerabilities in account_change.php in BtiTracker 1.4.1 and earlier allow remote attackers to execute arbitrary SQL commands via the (1) style or (2) langue parameter.
- Many more..

With Uila, you also have full visibility into the transactions for HTTP protocol. In this type of an attack, there will be No HTTP GET transaction before the POST transaction. In normal or valid web traffic, you would expect to see a GET before a POST. Also you will see shell commands to be executed by the webshell.



Uila Application Transaction Analysis

Uila's Threat Detection

To request a free trial for Uila, visit https://www.uila.com/uila-free-trial

INFO@UILA.COM WWW.UILA.COM +1-408-819-0777