OsservatoriO
AttacchInformatici

La crescente, quasi insostenibile, insicurezza dei sistemi informatici

DA SHELLSHOCK AGLI ANTIVIRUS

Marco R. A. Bozzetti,
OAI founder

Uno degli attacchi più significativi degli ultimi mesi del 2014, largamente pubblicizzato anche dalla stampa non tecnica, è Shellshock, identificato e classificato il 24 settembre 2014 nella banca dati CVE delle vulnerabilità come CVE 2014-7169 e CVE 2014-6271.
Può colpire sistemi Linux, Unix e OS X (sì,anche i sistemi Apple sono vulnerabili!) che utilizzino una versione della shell di comando Bash dal 4.3 in giù. La shell di comando Bash è una delle varie disponibili, e tra quelle frequentemente usate, per il mondo Unix/Linux. È anche un mezzo per invocare degli script.

Shellshock consente un'ampia varietà di attacchi da remoto, prevalentemente su web server con sistemi operativi Unix/Linux e che operano con script, ma anche tramite servizi quali Secure Shell (SSH) e con protocolli di rete Dhcp. Shellshock consente attacchi ai diritti d'accesso al sistema, in particolare di far eseguire comandi tipici da 'amministratore', ovviamente non essendolo ed agendo da 'attaccante'. La vulnerabilità di Linux Bash permette a un attaccante di eseguire qualsiasi tipo di comando sul sistema colpito. Per esempio, sfruttando la vulnerabilità di Linux Bash un attaccante può modificare il contenuto del web server, cambiare il codice del sito, rubare i dati dell'utente dal database, cambiare i permessi del sito, installare backdoor e così via. A rischio maggiore sono anche tutti i dispositivi dell'internet delle cose (sempre più spesso indicato solo mcon l'acronimo IoT), che utilizzano per la maggior parte Linux.
L'ulteriore criticità di Shellshock è data dalla difficoltà di scoprire tutti i vettori di attacco usati: in complesso quindi esso ha, o può avere, impatti ed effetti simili a quelli di Heartbleed.0

© vege - Fotolia.com

Come capire se si è stati colpiti da Shellshock

Si è già evidenziato come una delle sue criticità sia la difficoltà di individuarlo. La prima misura da adottare è usare una versione di Bash dal 4.4.
Nel caso si avesse la versione vulnerabile, dal 4.3 in giù, analizzando i web server logs potrebbero comparire segni come '()' o '{' , che sono indicatori di un possibile

OAI 2014

Stiamo procedendo alla realizzazione della quinta edizione dell'Osservatorio Attacchi Informatici, OAI 2014. Numerose le novità, tra queste:

- la copertura sia dell'anno 2013 che dell'intero 2014. Nelle edizioni precedenti l'ultimo anno considerato, quello della pubblicazione, era coperto solo fino al primo quadrimestre o al primo semestre. Il coprire l'intero ultimo anno porta a pubblicare il rapporto finale a marzo dell'anno successivo, ossia del 2015. Editore Soiel International;
- l'attivazione di un autorevole Comitato Scientifico OAI, che ha il compito di garantire e verificare la qualità e l'autorevolezza dell'indagine, dal questionario fino al rapporto finale;

Il Questionario OAI 2014 è disponibile per compilazione al seguente indirizzo:
http://www.malaboadvisoring.it/index.php?option=com_content&view=article&id=63&Itemid=79.

Compilate il Questionario 2014 e 'passate parola' ai colleghi di altre aziende/enti di ogni settore e dimensione: più risposte saranno disponibili, più autorevoli e significative saranno le indicazioni fornite dal Rapporto finale.

attacco. Altri errori potrebbero essere loggati in error_log.
In Internet sono disponibili anche gratuitamente alcuni programmi software che permettono di verificare se si è stati colpiti da Shellshock.

Antivirus: ma quanto sei sicuro ed efficace?

Già in alcuni passati articoli di questa rubrica si è evidenziato il fatto di come alcuni prodotti di antivirus (AV), piuttosto diffusi anche in Italia, presentassero alcune vulnerabilità, e fossero quindi 'insicuri'.
Gli antivirus dovrebbero rappresentare pertanto uno dei primi mezzi di contrasto e la loro efficacia è determinante per la sicurezza informatica. Ma quanto sono realmente efficaci? Sul tema un recente articolo dell'esperto Ken Munro tratta delle prestazioni degli antivirus, ovvero quanti virus essi sono in grado di individuare, soprattutto quelli più recenti.
L'autore, con la sua struttura, ha esaminato 51 AV in commercio, e ha verificato con opportune tecniche, tra le quali l'uso di 'meta-exploit' e di 'packing', la capacità di ciascun AV di identificare virus anche 'camuffati'.
I risultati di una prima indagine, condotta nell'aprile 2013, erano risultati piuttosto preoccupanti.
Alcuni esempi:

- 33 AV su 51 hanno individuato Meterpreter reverse shell non packed.
- 37 AV su 51 hanno individuato Meterpreter reverse shell packed con UPX, uno degli strumenti disponibili in internet per effettuare packing.
- 17 AV su 51 hanno individuato come falso positivo, ossia come codice maligno, il corretto applicativo Windows notepad.exe, packed con UPX.
- 20 AV su 51 hanno individuato Meterpreter shell packed con PolyCryptPE, un altro strumento di packing disponibile.
- 3 AV su 51 hanno individuato Meterpreter shell packed con Veil-Evasion, altro strumento disponibile, ma con una specifica personalizzazione.

Ancor più preoccupante è però il fatto che Ken ha rifatto la stessa analisi un anno dopo con nuovi esempi di virus e con risultati non confortanti:

- 14 AV su 51, rispetto a 4 su 51 dell'anno prima, hanno individuato l'output di Meterpreter shell fornito a uno script VBA, Visual Basic for Applications, poi importato in un documento Office abilitato a usare macro.
- 33 AV su 51, rispetto a 19 su 51 dell'anno prima, hanno individuato Meterpreter shell packed con Hyperion, altro strumento disponibile.
- 29 AV su 51, rispetto a 10 su 51 dell'anno prima, hanno individuato Meterpreter shell packed con MoleBox, altro strumento disponibile.

Molti AV hanno registrato miglioramenti, ma nel complesso questi risultati indicano come sia relativamente facile nascondere agli AV un codice maligno con tecniche e strumenti liberamente disponibili su Internet. E questo è uno dei motivi per cui i codici maligni continuano a risultare, soprattutto in Italia, in testa agli attacchi più diffusi.

Marco R. A. Bozzetti, *OAI founder*
marco.bozzetti@malaboadvisoring.it