CHE COS'È UN ATTACCO WATERING HOLE

L'ESEMPIO DEL CASO REALE CFR CI PERMETTE DI CAPIRE COME FUNZIONANO I MODERNI ATTACCHI MIRATI

Marco Bozzetti, OAI founder

Con i termini 'watering hole attack', traducibile in 'attacco alla pozza d'acqua', si fa riferimento a quegli agguati che gli animali carnivori tendono alle prede che si avvicinano a una pozza d'acqua per dissetarsi. I termini utilizzati nel contesto della sicurezza informatica sono una chiara metafora per indicare un attacco mirato a utenti, le prede, che accedono e navigano in determinati siti web, tipicamente di organizzazioni molto influenti e autorevoli. Il predatore, sapendo che in quel sito la preda andrà, e probabilmente in determinati giorni, l'aspetta con le proprie armi per... divorarla.

Per molti anni, e in parte ancora oggi, i principali attacchi informatici hanno avuto come obiettivo in maniera massima gli utenti generici di siti popolari e molto visitati, come Google, Facebook, Amazon, CNN, e così via. Obiettivo di tali attacchi era, ed è, principalmente il furto dell'identità digitale del generico utente per utilizzarla al fine di scopi fraudolenti: prelievi dal conto corrente del malcapitato, acquisti on line con la sua carta di credito, e quant'altro.

I nuovi tipi di attacchi, come quelli watering hole, gli APT e il spear phishing, invece si focalizzano su specifiche tipologie di utenti e di programmi, ben noti agli attaccanti.

La logica dell'attacco watering hole si concentra su siti web, non usati da una gran massa di persone, ma da un numero di utenti relativamente limitato e portatori di interessi specifici, per i quali tali utenti stanno accedendo al sito attaccato: utenti che per la loro posizione e ruolo hanno informazioni riservate e spesso significative capacità economiche, e che pertanto sono di forte interesse per gli attaccanti. Una volta connesso al sito già manipolato dall'attaccante, il browser, il dispositivo dell'utente (dal pc al lap top, dal tablet allo smartphone) e la sessione con il sito web sono a loro volta attaccati per carpire informazioni dell'utente, tipicamente le sue identità digitali utili a compiere frodi. Acquisite le informazioni, normalmente vengono cancellate le tracce dell'attacco stesso.

Da attacchi di massa e generici, si passa quindi ad attacchi specifici a determinati ambienti visitati prevalentemente da un gruppo specifico di utenti.

Il caso CFR

Il watering hole rappresenta una relativamente nuova tipologia di attacco, che è bene conoscere per potersi difendere. A questo scopo, e a titolo esemplificativo, si propone il caso del sito del Council on Foreign Relations (www.cfr.org), un'associazione privata statunitense, apartitica, composta soprattutto da uomini d'affari e leader politici che studiano i problemi globali e possono/vogliono influenzare la definizione della politica estera Usa.

Tra la fine del 2012 e gli inizi del 2013 il sito web del CFR è stato attaccato, si suppone da hacker cinesi, in modo che si infettassero gli end-point dei visitatori con un malware e gli attaccanti potessero accedere alle informazioni e alle identità digitali dei malcapitati.

Nel caso CFR, il tipo di utenza è tipicamente fatta da lobbisti, giornalisti, persone che hanno interesse a condizionari i decisori delle politiche estere del governo. La prima fase dell'attacco fu sferrato il 21

dicembre 2012, nel periodo natalizio, quando gli staff di sicurezza informatica sono ridotti: questo ha consentito al malware di rimanere sul sito per un tempo non breve. I colpiti dal malware furono quindi 'solo' i nuovi visitatori che accedevano con un browser Internet Explorer v8 configurato per le lingue inglese, cinese, giapponese, coreano, russo. Gli attaccanti hanno inserito nel sito web un malware 'cavallo di troia' capace di sfruttare una vulnerabilità delle vecchie versioni (dalla 6 alla 8) del browser Microsoft.

Il sofisticato malware ha operato nel seguente modo:

1. Verifica del browser e della sua configurazione con un JavaScript;
2. Il codice maligno in JavaScript ha forzato un downoload di un file immagine (xsainfo.jpg) nella cache del browser usando una tecnica di attacco chiamata 'drive-by cache'.
3. Questo file immagine è il 'dropper', ossia il vettore che installa un codice maligno nell'end-point (pc, tablet, smatphone) per nascondersi ai sistemi antimalware; il file immagine viene decodificato come un DLL e archiviato nel folder %TEMP% sempre come una immagine .jpg.
4. Il malware JavaScript a questo punto attiva Flash di Adobe per sfruttare una vulnerabilità di Internet Explorer v8 e attivare un attacco 'heap spray'. Con questo termine si indica una tecnica utilizzata per facilitare l'esecuzione di codice maligno: viene inserita una sequenza di byte nella memoria, per esempio cache, di un programma attivo, per esempio il browser;
5. L'end-point, pc o tablet o smartphone, è ora infettato e può iniziare l'individuazione ed il furto delle informazioni dell'utente.
6. Il malware in JavaScript non ha ancora finito il suo compito: per infettare altri nuovi utenti, mette in esecuzione il codice binario dal file 'shiape.exe' posto nel folder %TEMP%. Questo programma effettua un 'code injection' nell'eseguibile del browser, iexplore.exe, e si installa come file di programma modificando il registro del computer. Il codice maligno si registra come 'DirectDB.exe' e ad ogni nuovo login di utente infetta il suo browser come già descritto.

Cosa bisogna fare

Questa breve descrizione fa capire la sofisticazione e la complessità di un tipico attacco watering hole, che presuppone l'inserimento del codice maligno sul server del sito web in modo tale che sia difficile da scoprire. Nel caso CFR è stata usata una backdoor, il codice è stato camuffato, da immagine, e sono stati creati diversi file (oggetti multipli) con codice maligno, così da rendere più difficile la loro complessiva individuazione. I tradizionali e diffusi metodi di difesa, come gli antivirus, non risultano sufficienti a individuare e contrastare questo tipo di attacco.

La vulnerabilità zero-day di IE v8 è stata classificata CVE-2012-4792 e a fine dicembre 2012 Microsoft ha rilasciato un 'security advisory'. Le versioni successive di IE non hanno tali vulnerabilità, e questo evidenzia come una delle prime regole di prevenzione sia aggiornare sistematicamente ogni programma software all'ultima versione rilasciata.

Altri strumenti e metodiche possono aiutare a individuare e contrastare simili attacchi. Tra queste:

- Sistematica analisi delle vulnerabilità per i propri ambienti informatici consultando le varie banche dati disponibili, in primis la CVE (Common Vulnerabilities and Exposures, cve.mitre.org) .
- Rafforzamento (hardening) della sicurezza all'end-point, per esempio non consentendo l'uso di plugin se non necessari.
- Analisi del traffico attraverso diverse metodiche e strumenti.
- Analisi del comportamento dei sistemi, in particolare degli end-point, per l'individuazione di questi tipi di attacchi: è un confronto tra un utilizzo in condizioni normali e uno con sistemi "sospetti".
- Uso di strumenti di mitigazione delle vulnerabilità.

Marco Bozzetti
marco.bozzetti@malaboadvisoring.it