

Hoffmann Forensic Challenge

Oplossingen en uitslag

Voordat we bekendmaken wie de uiteindelijke winnaars zijn, geven we eerst de oplossing van de challenge.

Vraag 1: Wie zijn de medeterroristen van Willem Z. en wanneer is de aanslag gepland?

In een van de plaatjes was met behulp van steganografie een tekstbestand verborgen. Hierin stonden de namen en andere gegevens van de 7 medeterroristen en de datum van de aanslag, namelijk 2 januari.

Het plaatje dat de verborgen tekst bevatte was handmatig in de niet-gealloceerde ruimte van het ext3 bestandssysteem geplaatst, en dus niet verwijderd zoals de meeste mensen dachten. Een manier om vast te stellen dat het bestand niet door het bestandssysteem op het image was geplaatst, was door te observeren dat er geen indirect block tussen de data zat. Op Ext2/Ext3 bestandssystemen is het 13e block een indirect block. Zo'n indirect block heeft een lage entropy-waarde en zou tussen een jpeg (hoge entropy) gedetecteerd kunnen worden. Dit was wel het geval geweest als het bestand op de normale manier op het mmc-kaartje was gezet en daarna met 'rm' was verwijderd. Hierdoor was het alleen met behulp van carven uit het image te halen, of door de data zelf specifiek te doorzoeken op extra data.

Het wachtwoord dat nodig was om het tekstbestand uit het plaatje te halen, was geschreven in het OpenOffice-document. Dit document was gemodificeerd door de eerste en de tweede byte te verwisselen, de derde en de vierde byte, enz. Dit kan met een enkele 'dd' regel, of zoals een aantal mensen gedaan hebben, met een kort scriptje.

Vraag 2: Wat is het doelwit van de aanslag?

Het doelwit van de aanslag was de Keukenhof in Lisse, zoals te zien in een plaatje van Google Maps. Op het eerste gezicht was dit plaatje incompleet, maar dit was niet het geval. In de inode voor

dit bestand was handmatig de grootte aangepast, waardoor het leek alsof dit plaatje kleiner was dan het werkelijk was. Bestands groottes worden binnen Ext3 opgeslagen in hexadecimale waarden in de inode. De vervalste grootte van het bestand was 37000 bytes (88900000 Hex Little Endian notatie). Niemand heeft de aangepaste inode en waarde specifiek uitgelegd en beschreven. Doordat de data gewoon aanwezig is, kan het bestand met behulp van carving uit het image gehaald worden, aangezien een carver niet naar de bestandssysteeminformatie kijkt. Ook was het mogelijk om door handmatig het image te onderzoeken het correcte eind van het bestand te vinden en dit met 'dd' eruit te halen. Mensen die alle data tussen de start en het eind van het plaatje met 'dd' uit het image gehaald hebben, hadden niet direct een correct plaatje, want in dat geval zit er juist wel een indirect block tussen de data.

Vraag 3: Voor ieder relevant bestand: Verklaar wat Willem Z. heeft gedaan om de data te maskeren voor derden.

Dit is reeds uitgelegd bij vraag 1 en 2. De meeste inzendingen hadden de juiste datum, medeterroristen en plaats, maar hadden meer moeite met deze vraag. In een echt onderzoek is het verklaren en onderbouwen van de resultaten minimaal net zo belangrijk als de resultaten zelf. Gelukkig doen de meeste mensen in de praktijk minder moeite dan Willem Z. om hun data te maskeren...

Vraag 4: Hoe ben jij, als forensisch onderzoeker, aan de bovengenoemde informatie gekomen.

De stappen in een forensisch onderzoek dienen indien nodig herhaald te kunnen wor-

den, zodat ze door derden geverifieerd kunnen worden. Dit betekent dat ze correct en duidelijk gedocumenteerd moeten worden.

Beoordeling

Om in aanmerking te komen voor de prijzen, moesten de gegevens van de terroristen en de aanslag in ieder geval goed zijn. Daarbuiten hebben we nog op 4 gebieden beoordeeld:

1. Hoe goed heeft de onderzoeker verklaard wat voor acties Willem Z. heeft genomen om de gegevens te verbergen.
2. Hoe volledig was het onderzoek en hoe leesbaar was het rapport. Denk hierbij aan de volgende punten:
 1. Is de correctheid van het aangeleverde image geverifieerd, bijvoorbeeld met 'ewfverify'.
 2. Is een duidelijk beeld gegeven van de inhoud van het image en bijgevoegde meta-informatie, bijvoorbeeld door 'ewfinfo' en 'mmls'.
 3. Is ook buiten de ext-3 partitie gekeken naar aanwezige informatie. Dit was niet het geval, maar moest zeker wel gecontroleerd worden.
 4. Zijn alle genomen stappen in het onderzoek herhaalbaar en duidelijk aangegeven in het onderzoek, bijvoorbeeld door het ad-verbatim overnemen van de uitgevoerde programma regels en de bijbehorende output.
 5. Is van alle genoemde bestanden die uit het image gehaald is ook de (correcte) md5sum toegevoegd.
3. Andere fouten zoals incorrecte uitspraken of foute conclusies zijn ook meegenomen in de beoordeling.
4. Als twee mensen exact dezelfde eindscore hadden gebaseerd op de bovengenoemde punten, dan is de datum van inzending bekeken. Dit was bij de drie winnaars niet het geval.

Winnaars

- **Eerste plaats:** *Mattijs van Ommeren*
- **Tweede plaats:** *Arjen Smit*
- **Derde plaats:** *Hans Heins*

Kijk op www.linuxmag.nl voor het *winnende rapport!* «