



indi-2008-010-020

Analyse van tweedehands harde schijven

Project	: SURFworks
Projectjaar	: 2008
Programmalijn	: Technologie scouting
Onderdeel	: Forensics
Activiteit	: 4.2
Deliverable	: Analyse van tweedehands harde schijven
Toegangsrechten	: publiek
Auteur(s)	: Jaap van Ginkel, Rogier Spoor
Externe partij	: n.v.t.
Opleverdatum	: 30-9-2008
Versie	: 1.0

Samenvatting

Naar schatting zijn 5% tot 20% van de pc's wereldwijd besmet met zogenaamde spyware, wormen, rootkits, virussen en/of andere kwaadaardige software. De laatste jaren is er vooral een toename geweest van het aantal pc's die met wormen en spyware besmet zijn geraakt. Deze wormen zorgen bijvoorbeeld voor de distributie van SPAM en/of aanvallen op legitieme websites (DoS-aanvallen). Spyware heeft als doel om zoveel mogelijk commercieel interessante informatie te vergaren op de pc waarop deze is geïnstalleerd. Voorbeelden hiervan zijn: gebruikersnaam en wachtwoord gegevens, creditcard gegevens, gevoelige informatie van de pc kopiëren om hiermee iemand te kunnen chanteren, reclame tonen aan de pc gebruiker die geld oplevert voor de maker van de spyware.

Dit onderzoek is een onderdeel van een groter project dat tot doel heeft om tot een ontwerp van een forensische analyse dienst te komen. Het idee van deze dienst is, dat wanneer een computer/server is gehackt, de harde schijf kan worden opgestuurd naar SURFnet voor automatische analyse. Als eerste stap in dit grotere project is besloten om meer inzicht te krijgen in de hoeveel kwaadaardige software die daadwerkelijk aangetroffen wordt op harde schijven. Dit om een helderder beeld te krijgen van de problematiek en de situatie "in het veld". In dit onderzoek zijn gebruikte harde schijven ingekocht op computerbeurzen, winkels en webwinkels. Vervolgens zijn deze harde schijven geanalyseerd met het doel te onderzoeken of er sporen van kwaadaardige software te vinden zijn. Een tweede doel van dit onderzoek was inzage te verkrijgen in hoe goed de harde schijven worden gewist, alvorens deze worden verkocht.

Doelstelling

De doelstelling van het deelproject is om op snelle wijze inzicht te verkrijgen in de data die op gebruikte harde schijven staat. Welk soort data zich bevindt op de schijven en zijn er sporen van kwaadaardige software aangetroffen?

Aanpak

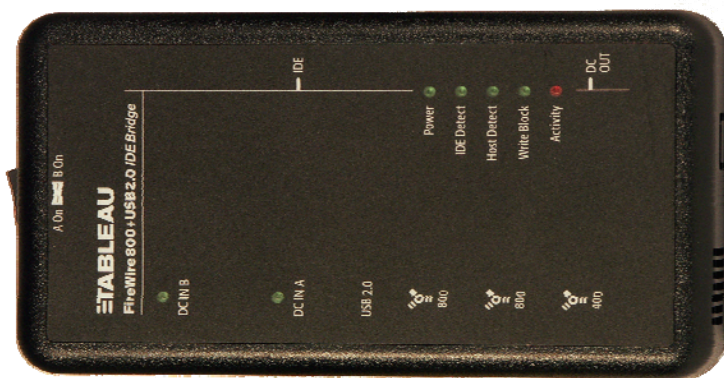
Er zijn bij 12 verschillende leveranciers in totaal 27 tweedehands harde schijven gekocht. Onder deze leveranciers waren partijen die via een webwinkel tweedehands hardware verkochten, partijen die op een computerbeurs stonden en partijen met uitsluitend een winkelpand. Er zijn niet alleen losse tweedehands harde schijven, maar ook complete tweedehands computers waar vervolgens de harde schijf uit verwijderd is alvorens het onderzoek werd gestart. De harde schijven zijn qua gebruik in te delen in de volgende groepen:

- Laptop harde schijven (2.5 ")
- Server harde schijven (SCSI)
- Werkstation harde schijven (ATA/SATA)

De schijven zijn met behulp van Forensics Toolkit 1.80 onderzocht. Om forensisch zuiver te kunnen werken is gebruik gemaakt van een writeblocker van het merk Tableau type: T3U voor SATA schijven en model T5 voor schijven met een IDE/PATA-interface. De schijven zijn handmatig onderzocht en vervolgens onderverdeeld in vier categorieën:

- Defecte Schijven die niet met eenvoudige middelen toegankelijk gemaakt konden worden
- Schijven die deskundig zijn gewist en daardoor geen leesbare relevante informatie meer bevatten
- Schijven die ondeskundig zijn gewist en daardoor nog wel leesbare informatie bevatten
- Schijven die niet gewist zijn en leesbare informatie bevatten

De schijven van de laatste twee groepen zijn aan een nader onderzoek onderworpen om meer inzicht te krijgen in de inhoud en de gebruikte software. Met behulp van hash sets van het NIST NSRL en van Accessdata KFF is gezocht naar bekende malware. Vervolgens is handmatig bepaald of deze malware ook werkelijk actief was.



Figuur 1 Gebruikte forensics writeblocker

Voor deze publicatie geldt de Creative Commons Licentie "Attribution-Noncommercial-Share Alike 3.0 Netherlands". Meer informatie over deze licentie is te vinden op <http://creativecommons.org/licenses/by-nc-sa/3.0/nl/>

Resultaten

Om privacy redenen zijn details van het onderzoek, die herleidbaar zijn tot de verkopende partij van de hardware en/of partij waarvan aantoonbaar data is aangetroffen op de hardware, achterwege gelaten. In totaal waren 10 harde schijven op deskundige wijze zodanig gewist dat er geen relevantie informatie meer aangetroffen kon worden met de forensische analyse.

Server harde schijven

Zeven schijven hadden diverse SCSI interfaces en konden door het ontbreken van een geschikte forensics bridge niet direct onderzocht worden. Met behulp van diverse losse (oude) scsi controllers is het uiteindelijk gelukt alle ruwe data over te zetten op een andere harde schijf, zonder de eventueel aanwezige data te beïnvloeden, waarna de data alsnog onderzocht konden worden. De resultaten hiervan zijn:

- 1 SCSI schijf was defect en toonde zichtbare sporen van oververhitting
- 2 SCSI schijven waren deskundig gewist de overige 4 bevatten data die toegankelijk gemaakt kon worden. Na een eerste onderzoek werd op 3 van de schijven Windows server operating system en 1 Linux operating system aangetroffen.
- Van de 4 leesbare SCSI schijven komen er twee uit een mirror set (RAID 1), deze bevatten dus identieke informatie, waarop de configuratie en data van een IIS webserver is aangetroffen, maar geen vertrouwelijke informatie.
- Van de overige 2 schijven bevat er één een database van een koepelorganisatie in de zorgsector. De andere bevat een eenvoudige IIS webserver installatie met weinig vertrouwelijke data.

Aantoonbare kwaadaardige software: niet aangetroffen

Werkstation harde schijven

In totaal zijn er 17 werkstation harde schijven onderzocht.

2 IDE schijven bleken defect en daardoor niet meer eenvoudig te onderzoeken. Van de overige 15 harde schijven waren er 6 waarop leesbare relevante informatie te vinden was. 3 van de 6 leesbare schijven zijn weliswaar gewist maar dermate ondeskundig dat vrijwel alle data op de schijf achterhaald kan worden.

Om een indruk te geven van de aangetroffen vertrouwelijke data een korte geanonimiseerde samenvatting:

- Een harde schijf van een studentenhuus bevatte de privé documenten van 8 verschillende studenten.
- Een harde schijf van de ICT afdeling van een internationale luchtvaartmaatschappij.
- Een schijf bevat vertrouwelijke data van een communicatieadviesbedrijf.
- Een aantal schijven bevat vertrouwelijke data van privé personen.
- Een IDE schijf is geschoond met een cleaning utility maar desondanks valt er uit de niet volledig gewiste registry nog informatie te halen die de voormalige eigenaar waarschijnlijk liever niet op straat heeft liggen.

- 3 van de 6 schijven bevatten een Windows XP OS
- 3 van de 6 schijven bevatten een Windows 9x OS

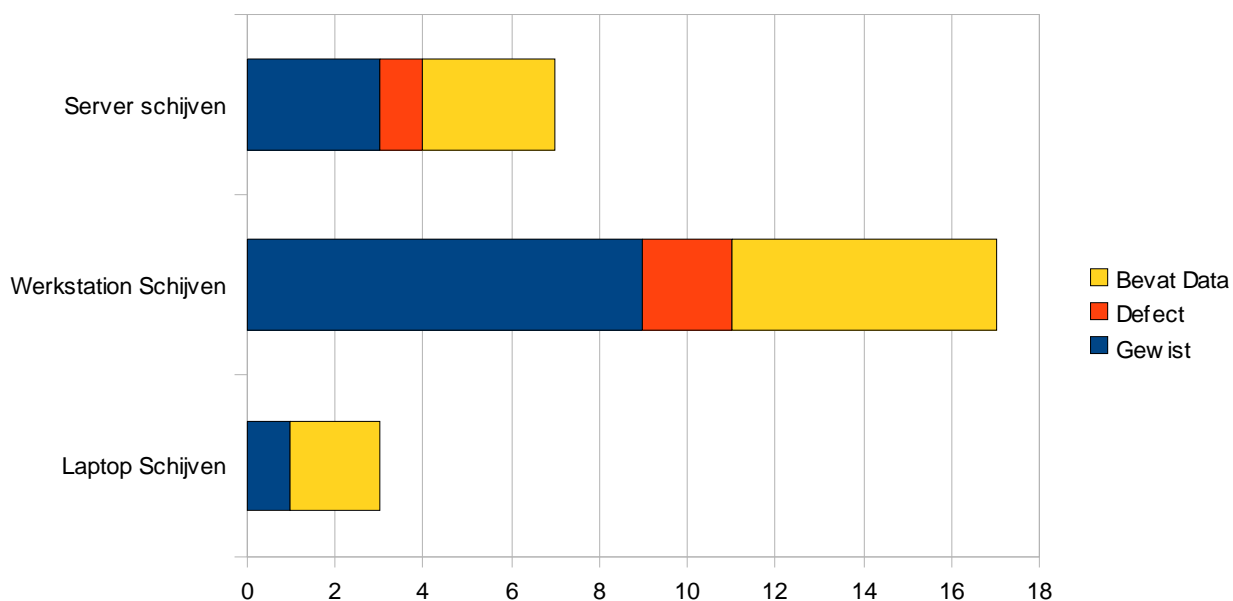
Aantoonbare kwaadaardige software:

- 1 van de 6 IDE schijven bevat een actief virus
- 1 van de 6 IDE schijven bevat een spyware keylogger
- 1 van de 6 IDE schijven bevatten mogelijk ongewenste browser helper object (BHO)

Laptop harde schijven (2.5 ")

Er zijn drie laptop harde schijven onderzocht, waarvan er twee data bevatten.

- 1 van deze 2 schijven, daarvan was getracht de data te wissen, maar dat is dermate ondeskundig gebeurd dat bijna alle informatie was terug te lezen. Op beide harde schijven is een Windows XP operating systeem aangetroffen.
- Een ondeskundig gewiste laptopschijf bleek van het senior management van een groot postbedrijf en bevatte vertrouwelijke strategiedocumenten en een volledig klantenbestand.
- Aantoonbare kwaadaardige software:
- 1 van de 3 laptop schijven bevatte mogelijk ongewenste browser helper object (BHO)



Figuur 1: Leesbare data op de schijven

Conclusie & Discussie

Het totaal aantal onderzochte harde schijven is te beperkt in omvang om een algemeen geldige uitspraken te kunnen doen, maar ze geven wel een duidelijk beeld aan over hoe bedrijven & particulieren omgaan met hun data, wanneer een computer is afgeschreven. Het is duidelijk dat circa de helft van de particulieren en bedrijven geen deugdelijke maatregelen neemt voor vernietiging van de aanwezige data op harde schijven. Hierdoor kan vertrouwelijke informatie alsnog in handen van derden vallen.

Qua kwaadaardige software is dit in de groepen werkstation- en laptop harde schijven gemiddeld voor 25% aangetroffen. Dit is, gezien de kleine omvang van de steekproef, waarschijnlijk een te hoog percentage, omdat het niet gesteund wordt door berichten van andere partijen. Desondanks maakt dit wel duidelijk dat er een probleem is. Vandaar dat er binnen dit SURFworks project in Q4 een ontwerp gemaakt zal worden voor een forensische dienst, waarmee grotendeels geautomatiseerde analyses gemaakt kunnen worden van computers. Dit met doel om bij calamiteiten een laagdrempelige dienst te kunnen aanbieden die een eerste orde forensische analyse kan uitvoeren van de computer.