Security: Malware

D. Leeuw

11 december 2023
v.0.8.0

Over dit Document

0.1 Leerdoelen

Dit document beschrijft de verschillende vormen van malware. Na bestudering van dit document heeft de lezer kennis van:

- Wat malware is
- Wat een 0-day expoit is
- Wat een virus is
- Wat een worm is
- Wat een trojan is en wat een botnet en kent de term zombie
- Wat spyware is
- Wat ransomeware is en wat een cryptolocker is
- Wat een rootkit is

0.2 Voorkennis

Voor een goed begrip van dit document is de volgende kennis gewenst:

- Kennis van de werking van computers met hardware, software en applicaties is gewenst.
- Kennis van het verschil tussen Unix-achtige systemen (Mac OS X en Linux) en Windows is gewenst.
- Voor het hoofdstuk ransomeware is voorkennis van PKI (public key infrastructure) gewenst.

Inhoudsopgave

Hoofdstuk 1

Wat is Malware

Malware is een samentrekking van Malicious (kwaadaardig) en Software. Het is een stuk software dat vaak niet of moeilijk detecteerbaar door de gebruiker draait op een operating system en waarvan de gebruiker niet weet dat het er is.

Malware wordt vaak "per ongeluk" geïnstalleerd. Er zijn veel aanvalsvectoren die gebruikt worden om malware op een computer te krijgen. De meest simpele vorm is dat een stukje extra code meekomt met wat lijkt op legale software. Versies van software waarvoor niet betaald hoeft te worden kunnen voorzien zijn malware.

Een andere techniek is via websites. Op een website kan verborgen (javascript) code zitten die een stukje malware installeert op de computer die de website bezoekt.

Een veel gebruikte techniek is via e-mail, waarbij er in de e-mail een executable zit die zich bijvoorbeeld voordoet als Word-document of als PDF, of waarin er een macro wordt gebruikt in een Word of Excel document. Ook een verwijzing naar een website met kwaadaardige code komt vaak voor.

Malware kent verschillende technieken van verspreiding en verschillende functionaliteiten. In dit document zullen we de meest voorkomende behandelen. Moderne malware maakt vaak gebruik van een combinatie van technieken om hun kans van overleven te vergroten.

1.1 Zero-day exploit

Malware maakt vaak gebruik van zwakheden in een operating system. Elk stukje software op een computer wordt geschreven door een programmeur en mensen maken fouten. Het zijn geen fouten die het programma

verhinderen om te draaien, of die voor de gebruiker merkbaar zijn, maar fouten die bijvoorbeeld te maken hebben met geheugenmanagement. Omdat de fouten niet de werking van het programma in de weg zitten zijn deze fouten vaak lastig om op te sporen. Het programma lijkt goed te functioneren en toch kunnen criminelen gebruik maken van deze fouten om het programma ook andere taken te laten uitvoeren.

Soms zijn security-analisten de criminelen voor en wordt er een security-update van de software uitgebracht voordat de criminelen het foutje vinden. Het analyseren van deze updates levert de criminelen dan weer veel informatie op over het foutje in de software zodat ze alsnog instaat zijn om systemen aan te vallen die geen updates hebben doorgevoerd. Het is daarom noodzakelijk om security-updates zo snel mogelijk door te voeren op systemen.

Het kan ook gebeuren dat criminelen een foutje ontdekken en gebruiken om in te breken op systemen voordat de de rest van de wereld van deze zwakheid weet. In zo'n geval spreken we van een 0-day exploit. Er zijn dus 0 dagen aan beveiliging voor deze exploit. De makers van de software moeten hard aan de slag om een oplossing te verzinnen en deze zo snel mogelijk vrijgeven om de gevolgen zoveel mogelijk te beperken.

Hoofdstuk 2

Virus

Een virus is een stukje code dat de mens nodig heeft om zich te verspreiden. Het is de code die hangt aan een PDF of een Word-document. De gebruiker moet de PDF openen om de code te activeren, als de gebruiker de PDF opslaat en niet opent of de PDF weggooit dan kan de code niets doen.

Code kan zich ook verspreiden via het downloaden van illegale programma's, of het delen van software met vrienden of vriendinnen.

Microsoft heeft in Windows een feature zitten waarbij CD's of USB-sticks automatisch starten (auto-run). Via deze feature kan ook kwaadaardige code gestart worden en zo kan een virus zich makkelijk van computer naar computer verspreiden.

Een virus wordt gestart door een gebruiker op het systeem en het virus draait dan ook met de rechten van die gebruiker. Als de Administrator een virus opstart heeft het virus dus ook Administrator rechten!

Hoofdstuk 3

Worm

Een worm lijkt erg op een virus, maar er zijn enkele verschillen. Een worm verspreidt zich via het netwerk en maakt gebruik van zwakheden in de netwerk-diensten of de netwerk-stack van een systeem. Een ander verschil met een virus is dat een worm zichzelf kan opstarten nadat het een systeem geïnfecteerd heeft. Waar een virus altijd de mens nodig heeft voor activatie heeft een worm éénmalig de mens nodig om op te starten daarna zoekt hij zelf zijn weg.

Wormen maken gebruik van zwakheden in de netwerk faciliteiten van een besturingssysteem. Het is dus geheel afhankelijk van welk proces er misbruikt wordt met welke rechten een worm kan draaien op een systeem. In het slechtste scenario draait de worm met rechten op kernel-niveau.

Hoofdstuk 4

Spyware

Spyware is zoals de naam al aangeeft software die informatie van een systeem verzamelt en deze doorgeeft aan de criminelen. Het kan gaan om e-mail adressen, toegangsgegevens zoals gebruikersnamen en wachtwoorden, maar ook om bank- en credit-card-gegevens.

De informatie wordt verzameld uit het adresboek en de e-mail software. Ook kan er een key-logger geïnstalleerd worden die vast legt wat een gebruiker intypt zodat gebruikersnamen en wachtwoorden of bankgegevens verzameld kunnen worden. Het gaat hierbij om het verzamelen van persoonlijke gegevens. De software die gebruikt wordt als spyware heeft dus voldoende rechten nodig om door de gebruiker gebruikt te kunnen worden.

Hoofdstuk 5

Ransomware

Een andere naam voor ransomeware is de vaak in de media gebruikte term cryptolocker. Ransomeware locked een computer en/of de bestanden om daarna de gebruiker te vragen om te betalen zodat de bestanden of de computer weer geunlocked kunnen worden. Het is niet gegarandeerd dat het betalen ook daadwerkelijk zorgt dat de bestanden weer toegankelijk worden, het gebeurt vaak dat er wel betaald wordt, maar dat de sleutel tot het unlocken niet geleverd wordt.

Cryptolockers maken gebruik van de public key infrastructure. De public key wordt gebruikt om de bestanden te encrypten. Na betaling hoop je de private key te krijgen om alle bestanden te decrypten. De rechten van de gebruiker waaronder de cryptolocker draait bepaalt waar de cryptolocker bij kan en welke bestanden er versleuteld kunnen worden. Alleen de bestanden waar de gebruiker schrijfrechten op heeft kunnen door de cryptolocker ge-encrypt worden.

Hoofdstuk 6

Trojan

Een trojan staat ook wel bekend als rat, remote access trojan. Dat laatste beschrijft het beste de functionaleit van een trojan. Het is een stukje software dat de criminelen de toegang tot een systeem verleent. Ze kunnen dus via een trojan commando's uitvoeren op een systeem. Wat dat betreft lijkt het erg op een remote administration tool.

De functionaliteit van een trojan is divers. Zo kunnen bijvoorbeeld de webcam en de microfoon bestuurd worden, maar kan de computer ook geconfigureerd worden zodat netwerk-verbindingen omgeleid worden of de machine kan lid gemaakt worden van een bot-net.

Om remote toegang tot het systeem mogelijk te maken moet een trojan een port open zetten waarop deze benaderd kan worden.

Meer informatie kan gevonden worden op de volgende websites:

- https://www.malwarebytes.com/blog/threats/remote-access-trojan-rat
- https://www.caldoo.nl/remote-access-trojans/

6.1 Botnet - Zombie

Als een crimineel een computer op afstand kan beheren, kan hij de computers ook onderbrengen in een cluster waarbij er bijvoorbeeld één commando naar 10 verschillende compters tegelijk gestuurd kan worden. Zo'n netwerk heet een botnet. Botnet is een afkorting van Robot Netwerk en de verschillende machines die de commando's uitvoeren worden zombies genoemd.

De zombies zijn geïnfecteerd door trojans en vaak wordt IRC (Internet Realy Chat) gebruikt om computers te koppelen in een groep. Deze groe-

pen kunnen bestaan uit duizenden computers waarmee bijvoorbeeld heel simpel een DDOS (Distributed Denial Of Service) attack uitgevoerd kan worden. Door namelijk elke computer een klein beetje netwerkverkeer naar een server te laten sturen zal de server uiteindelijk heel veel verkeer te verwerken krijgen, terwijl de zombies er zelf bijna geen last van ondervinden.

Hoofdstuk 7

RootKit

Root is de administrator op een Unix-achtige machine, bijvoorbeeld Mac OS X of Linux. Een root-kit zorgt ervoor dat de inbreker root-rechten krijgt of Administrator wordt op een Windowssysteem. Een inbreker moet dus met een account van een gebruiker zichzelf toegang verschaffen tot het systeem. Dit is vaak makkelijker dan direct inbreken op het administrator-account. De root-kit maakt gebruik van lokale zwakheden in het systeem om te zorgen dat de gebruiker root-rechten krijgt. Het is dus een twee-traps aanval, eerst inloggen als een gewone gebruiker en daarna voldoende rechten krijgen door gebruik te maken van een rootkit om te kunnen doen wat de crimineel wil doen.

De software wordt vaak geïnstalleerd op plekken zodat het minder snel gevonden kan worden of verbergt zichzelf als een verborgen proces.

Het verkrijgen van gebruikersnamen en wachtwoorden van systemen kan door het afluisteren van het netwerk, door social engineering of door inbraken op andere systemen waar wachtwoorden verkregen zijn die door een gebruiker ook gebruikt wordt op andere systemen.