Nutzen von Timelines im Incident Response

März, 2016

Klassifikation:
Öffentliche Version

IOprotect GmbH
Huobstrasse 14
8808 Pfäffikon SZ
+41 (0)44 533 00 05
info@ioprotect.ch
www.ioprotect.ch

Einleitung

Implementierte Schutzmassnahmen greifen nicht mehr im gewünschten Masse und Unternehmen sind vermehrt mit der Frage konfrontiert, wie Incident Response bei einem Verdacht auf einen Vorfall aussehen soll. Neben den notwendigen Vorbereitungen hinsichtlich Bereitstellung von Daten zur Analyse (z.B. Web Proxy Logs, Windows Event Logs), der Definitionen von Prozessen, Zuständigkeiten, Berechtigungen und Befugnissen sind auch die konkreten Analysemethoden entscheidend für ein erfolgreiches Incident Handling. Dieses Dokument soll einen Aspekt daraus näher beleuchten und die Möglichkeiten und den Nutzen von Timeline-Analysen an einem konkreten Fallbeispiel erörtern.

Fallbeispiel

Ein Mitarbeiter aus der Buchhaltung meldete sich beim IT-Support mit der Information, sein System verhalte sich seit einigen Tagen abnormal und die Harddisk sei ebenfalls viel aktiver und hörbarer als früher. Die Analyse der Antiviren-Logs brachte keine Erkenntnisse. Die ebenfalls in die Wege geleitete Analyse der Web-Proxy Logs zeigten offensichtlichen Verkehr, welcher zu einem Remote Administration Tool (RAT) gehört. Die Frage ob eine erfolgreiche Kompromittierung stattfand, war somit bereits beantwortet. Die Frage nach dem Angriffsvektor war jedoch nach wie vor nicht geklärt.

Analyse mittels Timeline

Ein mögliches Vorgehen, den ungeklärten Angriffsvektor ausfindig zu machen ist die Erstellung und Analyse einer Timeline. Diese kann ausschliesslich die Veränderungen (Zeitstempel) eines Dateisystems beinhalten oder weitere Zeitstempel und Angaben aus Windows Event Logs, Registry Einträgen, Browser Caches, Meta-Informationen von Dokumenten etc. Veränderungen, welche analysiert werden können, umfassen Erzeugung, Modifikation, Zugriff und Löschung von Elementen.

Erzeugen einer Timeline

Die Erzeugung einer Timeline auf einem Live-System führt dazu, dass gewisse Timestamps verändert werden (beispielsweise die Access-Time von Dateien). Je nach Situation kann dies unerwünscht sein und bedingt daher entweder eine forensische Kopie der Festplatte oder die Verwendung von Write-Blocker, die eine Veränderung auf der Festplatte verhindert. Es muss also früh im Prozess der Timeline Erzeugung entschieden werden, ob eine solche auf dem Live-System erstellt, oder zuerst eine forensisch korrekte Kopie des Systems angelegt wird. Diese Abschätzung und Entscheidung muss bei jedem Fall neu getroffen werden, abhängig von den konkreten Umständen, dem verfolgten Ziel des Incident Response, aber auch von den Ressourcen, welche für einen Fall zur Verfügung stehen (personell und finanziell). Einen weiteren Einfluss auf die Vorgehensweise hat auch die Konfiguration der Systeme. Ist eine Harddisk Verschlüsselung im Einsatz, so ist zusätzlicher Aufwand für eine Offline Analyse einzuplanen oder man beschränkt sich auf eine Live Analyse.

Analyse einer Timeline

Beim vorliegenden Fallbeispiel ergab sich eine Timeline, welche folgende Auffälligkeiten aufwies:

2015-11-27T08:03:29	[\Microsoft\Windows Portable Devices\Devices\WPDBUSENUMROOT#UMB#2&37C&0&STORAGE#VOL#_??_USBSTOR#DISK&VEN_&PROD_&REV_0.00#15&0#] FriendlyName: [REG_SZ] BLUEBOX
2015-11-27T08:03:29	[Empty description] File size: 8107 File attribute flags: 0x00000020 Drive type: 3 Drive serial number: 0x4815b80f Local path: C:\Users\john\Desktop\Infos.zip Link target: Infos.zip
2015-11-27T08:03:29	[\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.zip] Index: 1 [MRU Value 0]: Path: Infos.zip Shell item: [Infos.lnk]
2015-11-27T08:03:29	[\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}\Count] C:\Users\john\Desktop\infos.lnk: [UserAssist entry: 12 Count: 1 Application focus count: 0 Focus duration: 1]
2015-11-27T08:03:29	[\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count] Microsoft.AutoGenerated.{D8AF2BE3-19BC-1D86-5582-F9AA3A6F0913}: [UserAssist entry: 15 Count: 1 Application focus count: 1 Focus duration: 120027]
2015-11-27T08:03:29	Prefetch [POWERSHELL.EXE] was executed - run count 1 path: \WINDOWS\SYSTEM32\WINDOWSPOWERSHELL\V1.0\POWERSHELL.EXE hash: 0x59FC8F3D volume: 1 [serial number: 0x4815B80F device path: \DEVICE\HARDDISKVOLUME1]
2015-11-27T08:03:29	TSK:/Users/john/Desktop/infos.lnk
2015-11-27T08:03:29	Location: http://www.evil.tld/send/info.php Number of hits: 1 Cached file: R3V6J9FZ\info[1].htm Cached file size: 393 HTTP headers: HTTP/1.1 200 OK
2015-11-27T08:03:29	Prefetch [HOSTNAME.EXE] was executed - run count 1 path: \WINDOWS\SYSTEM32\HOSTNAME.EXE hash: 0xA62916AE volume: 1 [serial number: 0x4815B80F device path: \DEVICE\HARDDISKVOLUME1]

Damit konnte der Infektionsvektor via USB-Stick klar aufgezeigt werden. Diese Infektion fand mit Hilfe des Mitarbeiters statt, der ein LNK-File[1] innerhalb eines ZIP-Archives startete. Vom Ablauf her zeigt sich schön, dass basierend auf dem LNK-File ein Powershell Script ausgeführt wurde, kurz danach ein Webzugriff erfolgte, welcher wiederum zu einem weiteren Aufruf eines Programms (hostname.exe) führte.

Tools

Nebst kommerziellen Forensic Frameworks, welche die Erstellung von Timelines unterstützen, bieten sich für den Einsatz auch Applikationen aus dem Open-Source Bereich an. Zu nennen sind an dieser Stelle:

- Autopsy: http://www.sleuthkit.org/autopsy/timeline.php
- Plaso / Log2timeline: https://github.com/log2timeline/plaso/wiki
- TimeSketch: http://www.timesketch.org/

Schlussbemerkung

Bei Interesse zu weiteren Details von Timeline Analysen oder weiteren Themen rund um Incident Response und Incident Handling stehen Ihnen die Experten von IOprotect gerne zur Verfügung.

[1] Die Gefahr von LNK Files: http://www.ioprotect.ch/download/Risiko_LNK_Files.pdf