Vírusmentesítés naplóelemző eszközökkel

Esettanulmány

Hétpecsét Információbiztonsági Egyesület

Információvédelem menedzselése LIX. Szakmai fórum

Szabó László

BalaBit IT Kft.

Service Delivery and Training Manager

szabo.laszlo@balabit.hu

2014. január 15.

Esettanulmány leírás

Esettanulmány leírás

Helyszín:

- Budapest, egy magyar közigazgatási intézet informatikai hálózata

Mikor?

- 2009. április 25 – 30.

Környezet leírása:

- Túlnyomórészt Windowsos hálózat:
  - 80-100 szerver (Windows 2003, Linux, ISA tűzfal, Cisco ASA, IDS)
  - 800-1000 kliens (XP, Vista)
  - Központi menedzselésű antivirus rendszer

Esettanulmány leírás

Mi történt?

- Lassú hálózat
- A felhasználók nem tudnak bejelentkezni a hálózatba
- A szerverszolgáltatások elérhetetlenné váltak
- „Kőműves Kelemen jelenség”

A mi feladatunk:

- A fertőzés gócpontjának megtalálása
- Az újrafertőződés meggátolása
- „Root cause analysis„
- *Titkos záradék: a fertőzés kiindulási okának feltárása*

Esettanulmány leírás

A nyomozatról:

- Elérhető incidens-jelentések áttanulmányozása
  - *A vírusvédelmi rendszert szállító cég bevonása a 0. percben megtörtént*
  - *A túlterhelés megszüntetése érdekében a nem kritikus szolgáltatásokat futtató szerverek leállításra kerültek*
  - *A vírus analizálása és eltávolítása az észlelést követően azonnal megkezdődött*
- Rendelkezésre álló naplóállományok begyűjtése és elemzése
- Sérülékenységvizsgáló scanek futtatása
- Ideiglenes központi naplózószerver üzeme helyezése
- Javaslatok megtétele és ellenintézkedések meghozatala
- Összefoglaló dokumentáció az eset leírásával és a javaslatokkal

Esettanulmány leírás

A nyomozatról - a vírus karakterisztikája:

Név: Worm:Win32/Conficker.A (majd B,C,D variánsok)

Megjelenés: 2008-11-25

Terjedés: LAN/WAN hálózaton, weben, vagy hordozható meghajtókon gyenge jelszavak törésével és az MS08-067 sérülékenységen keresztül

A fertőzés jelei:

- Bizonyos IT biztonsággal kapcsolatos weboldalak elérését blokkolja
- A felhasználók nem tudnak bejelentkezni (kitiltódnak az AD-ból)
- Erős forgalmazás a TCP445 – ös porton keresztül (MS -DS, AD, Windows Share-ek)
- admin$ sharek elérését letiltja (ill. azokon terjed)
- Autorun.inf fileok találhatóak a kukában
- Az alábbi fájlokat tölti le a webről a háttérben:
  http://trafficconverter.biz/4vir/antispyware/loadadv.exe
  http://www.maxmind.com/download/geoip/database/GeoIP.dat.gz

Esettanulmány leírás

A nyomozatról - a vírus karakterisztikája:

Név: Worm:Win32/Conficker.E

Megjelenés: 2009. április *(Az incidens időpontjában még ismeretlen!)*

Tevékenység:

Ugyanaz mint a korábbi variánsok plusz:

- A Win32/Conficker.X féreg véletlenszerűen kiválasztott UDP/TCP portokon nyit hátsóajtót.

- Fájlokat próbál meg letölteni az Internetről. Az URL címeket véletlenszerűen generálja.

Esettanulmány leírás

A nyomozatról – vizsgált naplók:

Windows naplók (DC)

- 529 Windows Security Eventek (Hibás felhasználónév vagy rossz jelszó)
- 644 Windows Security Eventek (Felhasználói fiók zárolva)

CISCO logok (ASA, switchek)

- CiscoWorks verziója elavult
- Az átirányított IDS és tűzfal-logok nem érkeztek meg
- A CISCO ASA-n csak az elutasított csomagok logolódnak
- A switcheken nincs forgalom-naplózásra lehetőség

Esettanulmány leírás

A nyomozatról – vizsgált naplók:

Központi naplózószerver

- KIWI syslog for Windows

- A futtató Windows a támadás első napján fertőzést kapott és le kellett állítani

- Az IDS ill. tűzfal-logok ide sem érkeztek meg

MS ISA szerver (proxy)

- Elemzésük során jól látszanak a fertőzött IP-címek

- Statisztikai és idősor-elemzéssel analízissel remekül elkülöníthetőek a szokatlan események, köztük a féreg jellemzői

Antivirus-rendszer naplói

- Érdemi információt nem találtunk bennük

Vírusmentesítés naplóelemző eszközökkel


```
#Software: Microsoft Internet Security and Acceleration Server 2004
#Version: 2.0
#Date: 2009-04-25 00:00:00
#Fields: computer       date    time    IP protocol     source  destination     original client IP      source network  destination network      action  status  rule
application protocol    bidirectional   bytes sent      bytes received  connection time source name      destination name        username        agent   interface
IP header
-       2009-04-25      00:05:48        TCP     172.17.250.20:4880      81.93.193.198:47645     172.17.250.20   Internal        External        Terminate
0x80074e20      Enged. kim. forg.       Unidentified IP Traffic Y       144     0       70000   -       -       -       -       -       -
-       2009-04-25      00:05:48        TCP     172.17.250.20:4882      79.121.15.144:34346     172.17.250.20   Internal        External        Terminate
0x80074e20      Enged. kim. forg.       Unidentified IP Traffic Y       144     0       70000   -       -       -       -       -       -
-       2009-04-25      00:05:48        TCP     172.16.240.156:139      192.168.77.70:4827      172.16.240.156  Internal        Internal        Denied
0xc0040017      -       Unidentified IP Traffic N       0       0       -       -       -       -       -       192.168.112.253 45 00 00 30 0a 9b 00 00 7f 06 86 91 ac
10 f0 9c c0 a8 4d 46
-       2009-04-25      00:05:48        TCP     172.16.240.156:139      192.168.77.70:4810      172.16.240.156  Internal        Internal        Denied
0xc0040017      -       Unidentified IP Traffic N       0       0       -       -       -       -       -       192.168.112.253 45 00 00 30 0a 9c 00 00 7f 06 86 90 ac
10 f0 9c c0 a8 4d 46
-       2009-04-25      00:05:48        UDP     172.17.250.20:57297     99.233.116.151:55389    172.17.250.20   Internal        External        Establish       0x0
Enged. kim. forg.       Unidentified IP Traffic Y       0       0       -       -       -       -       -       -
-       2009-04-25      00:05:48        UDP     172.17.250.20:57297     89.47.154.116:62949     172.17.250.20   Internal        External        Terminate
0x80074e23      Enged. kim. forg.       Unidentified IP Traffic Y       131     305     6000    -       -       -       -       -       -
-       2009-04-25      00:05:48        UDP     172.17.250.20:57297     84.73.180.193:49034     172.17.250.20   Internal        External        Establish       0x0
Enged. kim. forg.       Unidentified IP Traffic Y       0       0       -       -       -       -       -       -
-       2009-04-25      00:05:48        UDP     172.17.250.20:57297     59.94.254.152:60787     172.17.250.20   Internal        External        Establish       0x0
Enged. kim. forg.       Unidentified IP Traffic Y       0       0       -       -       -       -       -       -
-       2009-04-25      00:05:48        UDP     172.17.250.20:57297     122.53.6.245:29611      172.17.250.20   Internal        External        Terminate
0x80074e23      Enged. kim. forg.       Unidentified IP Traffic Y       131     305     6000    -       -       -       -       -       -
-       2009-04-25      00:05:48        UDP     172.17.250.20:57297     67.8.233.192:62281      172.17.250.20   Internal        External        Establish       0x0
Enged. kim. forg.       Unidentified IP Traffic Y       0       0       -       -       -       -       -       -
-       2009-04-25      00:05:48        UDP     172.17.250.20:57297     68.241.147.8:63609      172.17.250.20   Internal        External        Terminate
0x80074e23      Enged. kim. forg.       Unidentified IP Traffic Y       131     305     6000    -       -       -       -       -       -
-       2009-04-25      00:05:48        UDP     172.17.250.20:57297     74.220.166.186:43404    172.17.250.20   Internal        External        Establish       0x0
Enged. kim. forg.       Unidentified IP Traffic Y       0       0       -       -       -       -       -       -
```

Esettanulmány leírás

Okok:

- Gyenge jelszópolicy, túlzottan megengedő üzemeltetési/biztonsági szabályok
- Központi frissítés hiánya, hiányzó MS javítócsomagok
- Nem szegmentált hálózat
- Központi monitoring ill. naplómenedzsment hiánya
- Szakértelem hiánya (kockázatvállalás/szolgáltatáskiesés)
- A vírusvédelmi rendszer számára ismeretlen vírusvariáns

„Legjobb gyakorlat”

Ellenőrzőlista - Naplóbejegyzések ellenőrzése biztonsági incidensek felderítéséhez

Critical Log RevieW CHECKLIST for Security Incidents
Authored by Anton Chuvakin (chuvakin.org) and Lenny Zeltser (zeltser.com). Reviewed by Anand Sastry. Distributed according to the Creative Commons v3 "Attribution" License.
Cheat sheet version 1.0.

This cheat sheet presents a checklist for reviewing critical logs when responding to a security incident. It can also be used for routine log review.

General Approach

1. Identify which log sources and automated tools you can use during the analysis.
2. Copy log records to a single location where you will be able to review them.
3. Minimize "noise" by removing routine, repetitive log entries from view after confirming that they are benign.
4. Determine whether you can rely on logs' time stamps; consider time zone differences.
5. Focus on recent changes, failures, errors, status changes, access and administration events, and other events

Security tool logs (e.g., anti-virus, change detection, intrusion detection/prevention system)
Outbound proxy logs and end-user application logs
Remember to consider other, non-log sources for security events.

Typical Log Locations

Linux OS and core applications: /var/logs
Windows OS and core applications: Windows Event Log (Security, System, Application)
Network devices: usually logged via Syslog; some use proprietary locations and formats

What to Look for on Linux

Successful user login	"Accepted password", "Accepted publickey", "session opened"
Failed user login	"authentication failure", "failed password"
User log-off	"session closed"
User account change or deletion	"password changed", "new user", "delete user"
User logon/logoff events	Successful logon 528, 540; failed logon 529-537, 539; logoff 538, 551, etc
User account changes	Created 624; enabled 626; changed 642; disabled 629; deleted 630
Password changes	To self: 628; to others: 627
Service started or stopped	7035, 7036, etc.
Object access denied (if auditing enabled)	560, 567, etc

What to Look for on Network Devices

Look at both inbound and outbound activities.
Examples below show log excerpts from Cisco ASA logs; other devices have similar functionality.

Traffic allowed on firewall	"Built ... connection", "access-list ... permitted"
Traffic blocked	"access-list ... denied",

Vírusmentesítés naplóelemző eszközökkel

TOP 7 Riport – Nem(csak) menedzsereknek

1. Autentikációs és Authorizációs Riportok

Pl: a) Bejelentkezési kísérletek (sikeres, sikertelen) letiltott/szerviz/nem létező/alapértelmezett/felfüggesztett accountra vonatkozóan.

b) Kiemelt jogosultság használatának riportja, (su, sudo, Futtatás mint, stb. (sikeres, sikertelen)

2. Változások riportjai

Pl: a) Felhasználók ill. felhasználói csoportok létrehozása/módosítása/törlése

b) Adminisztrátori ill. kiemelt jogosultságú felhasználók létrehozása

TOP 7 Riport – Nem(csak) menedzsereknek

3. Hálózati forgalmi riportok

Pl: a) Keletkező naplók mennyiségének trendje

b) Belső IP címek, amelyek több különböző porton, protokollon kommunikálnak

4. Erőforrások hozzáférésének riportjai

Pl: a) Toplista a blokkolt webes forgalmakról (malware, felnőtt tartalom, stb.)

b) Top adatbázis felhasználók hozzáférései (az ismert alkalmazások kivételével)

Vírusmentesítés naplóelemző eszközökkel

TOP 7 Riport – Nem(csak) menedzsereknek

5. Malware riportok

Pl: a) Észlelt, de el nem távolított vírusok riasztásai

b) Minden anti-virus rendszerrel kapcsolatos probléma (összeomlás, leállítás, frissítési hiba, stb.)

6. Figyelmeztetések és rendszerhibák

Pl: a) Kritikus hibák rendszerenként

b) Kapacitásproblémák (mem, CPU, diszk, stb.)

TOP 7 Riport – Nem(csak) menedzsereknek

7. Analitikus riportok – NBS (Never Before Seen) események

Pl: a) ÚJ Log típusok, esemény típusok

b) ÚJ Sikeresen authentikáló felhasználók

c) ÚJ Kiemelt jogosultsággal kapcsolódó forráscímek listája

d) ÚJ Külső címekre forgalmazó belső IP címek

e) ÚJ Kapcsolódás eddig nem ismert portokra a belső hálózaton

Összefoglalás

Jótanácsok:

- Sosem késő elkezdeni! (Ma sem...)

- Minden az alapokon múlik!

- Mindenkinek vannak logjai! → Kezdeni kell velük valamit! → Erre való a Logmenedzsment!
  Indulj a Logmenedzsmentből, és innen haladj a SIEM felé!

- Egyszerű elemzéssel gyors (ámbár limitált) eredmények érhetőek el!
  Fókuszálj a konkrét problémák megoldására!

- A fejlettebb elemzés hatékonysága nem a vásárolt rendszer tudásán múlik, hanem a pontos igénymeghatározástól függ!

- „A kevesebb néha több...”

Köszönöm a figyelmet!

Szabó László

BalaBit IT Kft.

Service Delivery and Training Manager

szabo.laszlo@balabit.hu