MRLAB

FAT32 (file allocation table) autorun virusları və qorunma mexanizmi

Azərbaycan Respublikası Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidməti – Kompüter İnsidentlərinə qarşı Mübarizə Mərkəzi - Malware Research Lab – S. Abasov - 16 Aprel 2022

Bir zamanlar olduqca populyar olan bu viruslar günümüzdə artıq populyarlıqlarını itiriblər. Bu məqalədə sizlərə Microsoftun Windows əməliyyat sisteminə gətirdiyi təhlükəsizlik politikası ilə öncəki məşhurluğunu itirən AutoRun (AutoPlay) viruslarınından əsas qorunma mexanizmi üzərinə danışacağıq.

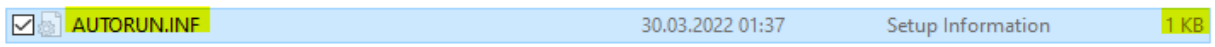
AutoPlay funksionallığı əslində Windows əməliyyat sisteminin istifadəçilərin rahatlığı üçün hazırlanmış bir mexanizm idi. Lakin 3-cü tərəf bu mexanizmi yayılmaq üçün istifadə etməyə başladı. Windows XP əməliyyat sistemi ilə gələn bu funksionallıq sistemdə mount edilən sürücülər içərisində autorun.inf faylını parse edərək buna uyğun növbəti əməliyyatı icra edirdi. AutoRun viruslarında əksər hallarda bu əməliyyat sürücü içərisində olan executable faylını icra etmək idi. Burada əsas problem bu əməliyyatı iştifadəçinin icazəsi olmadan icra edilməsi idi. Beləliklə yoluxmuş sürücü daxil edilərkən sistem avtomatik olaraq sürücüdə gizli şəkildə saxlanılan virusu icra etməyə başlayırdı. Sürücülər necə yoluxdurulurdu? Sürücülərin yoluxdurulması üçün ilk öncə komputerin yoluxdurulması lazım idi. Beləki öncədən hər hansl bir yol ilə yoluxmuş komputerdə fəaliyyət göstərən virus **Device Change Notification** qəbul edirdi. Komputerə hər hansı removable sürücü daxil edildiyi təqdirdə virus bu haqda notification alırdı və həmin sürücü içərisinə 2 ədəd fayl yazırdı.

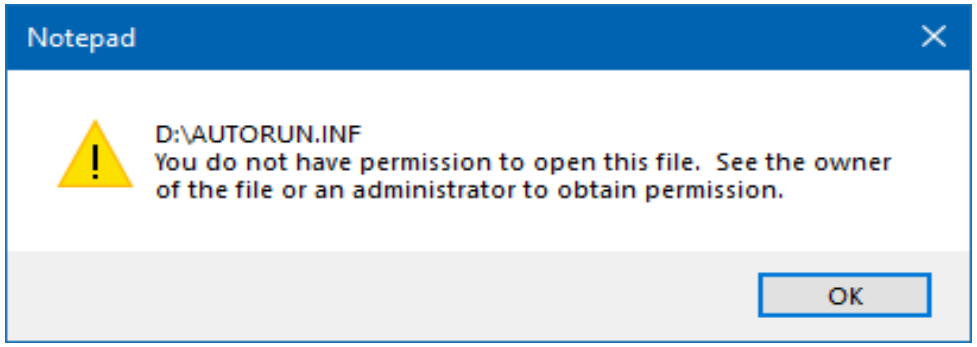
Bunlardan biri *autorun.inf* digəri işə sürücünün daxil ediləcəyi başqa komputerdə icra edilməsini istədiyi *executable fayl*. Fayllar sürücüyə yazıldıqdan dərhal sonra gizli fayl atributları set edilərək faylların normalda görünməsinin qarşısı alınırdı. Beləliklə artıq yoluxmuş sürücü başqa komputerlərə insert edildiyi zaman virus avtomatik şəkildə işə düşür və komputerı yoluxdururdu. Bundan sonra virus eyni şəkil yeni komputerdədə yuxarıdakı əməliyyatları icra edərək özünə yeni hədəflər seçirdi. Bu ailədən olan virusların ən populyar örnəkləri Conficker, Sality vs idi.

```
[autorun]
open=setup.exe
icon=setup.exe,0
label=My install CD
```

Beləliklə yoluxma sayı artdığı üçün Microsoft bu mexanizmin fəaliyyəti üçün bəzi limitlər gətirdi. (**CD/DVD-ROM** - sürücülər istisna).
Artıq istifadəçilərə Windows Registry üzərindən AutoRun mexanizmini blok etmə imkanı tanınırdı. Lakin buna qədər artıq bir neçə təhlükəsizlik kompnyası AutoRun virusları ilə effektiv mübarizə metodu işləyib hazırlamışdılar. Beləki bu metod vasitəsi ilə sürücü içərisinə normal viruslar kimi autorun.inf faylı yazılırdı. Lakin digərlərindən fərqi bu fayl silmək mümkün deyil idi. Nəticədə yoluxmuş komputerə daxil edilən bu sürücüyə virus autorun.inf faylını yazmaq istədiyi halda sistem error verir və faylı yarada bilmədiyi haqda məlumat verirdi. Bu metod diqqətimi cəlb etdiyi üçün məlumat almağa çalısamda bu haqda məlumat tapa bilmediyim üçün qərara gəlmişdim ki, özüm kiçik bir analiz aparım və əslində nəyin baş verdiyini anlayım.
Bunun həmin zamanlar məşhur olan Panda Security məhsulu "**Panda USB Vaccine**" proqram təminatını test etmişdim.

Sürücü içərisində gizli fayl olaraq yalnız autorun.inf faylı görünürdü. Fayla access almaq (**read**, **write**, **delete**) istədikdə isə sistem bizə permission error verərək fayla baxmaq icazəmizin olmadığı mesajı verirdi.





Lakin sistem error verdiyi üçün təxmin edə bilirdim ki, məsələ **FAT32.sys** faylının diski parse etməyindən irəli gəlirdi. Buna görədə nə baş verdiyini anlamaq üçün diski manual olaraq parse etmək qərarına gəldim. İlk öncə FAT32 fayl sistemi (struktur) spesifikasiyasına göz gəzdirdim. Diski parse etməyim üçün vacib idi.
Ətraflı: https://www.win.tue.nl/~aeb/linux/fs/fat/fatgen103.pdf
FAT fayl sistemi **4** əsas sektordan ibarətdir.

A FAT file system volume is composed of four basic regions, which are laid out in this order on the volume:

0 – Reserved Region
1 – FAT Region
2 – Root Directory Region (doesn't exist on FAT32 volumes)
3 – File and Directory Data Region

Bundan sonra ki, əməliyyatlar üçün Python dilində kiçik bir script yazaraq parse əməliyyatını avtomatlaşdırdım. Tamamı ilə boş disk üzərində işlədiyim üçün FAT32 fayl sistemini tam parsing etməyə ehtiyyac yoxdur. Burada əsas məqsəd faylların yerləşdiyi **RootDir** sektoruna keçməkdir. Bunun üçün spesifikasiya bizə aşağıdaki şəkildə düstur verib.

```
RootDirSectors = ((BPB_RootEntCnt * 32) + (BPB_BytsPerSec – 1)) / BPB_BytsPerSec
```

Note that on a FAT32 volume the BPB_RootEntCnt value is always 0, so on a FAT32 volume RootDirSectors is always 0.

RootDirSectors = 0
Bizə lazım olan məlumatlar **FirstDataSectorda** yerləşir. Offseti aşağıdaki düstür ilə hesablayırıq.

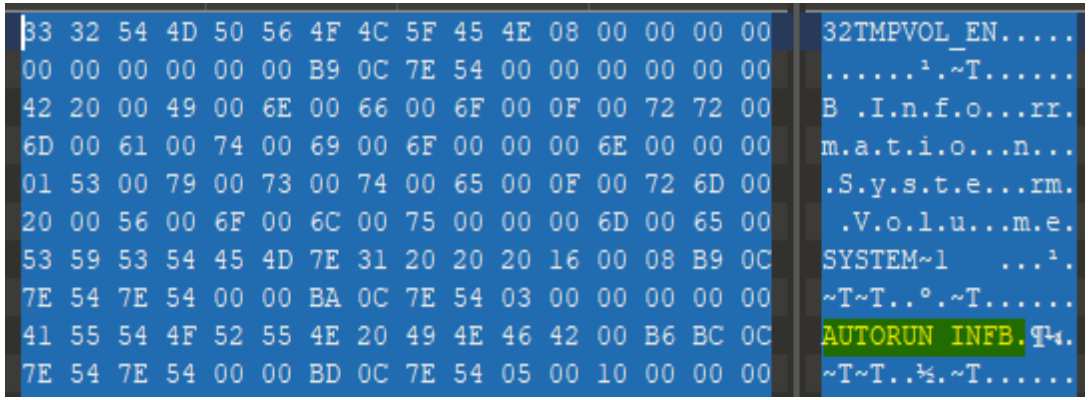
```
If(BPB_FATSz16 != 0)
    FATSz = BPB_FATSz16;
Else
    FATSz = BPB_FATSz32;

FirstDataSector = BPB_ResvdSecCnt + (BPB_NumFATs * FATSz) + RootDirSectors;
```

Figure 1 FirstDataSector offset hesablama düsturu

Aşağıda ki, kodun köməkliyi ilə data sectorun offsetini tapdım.

```
f = open(r"\\.\D:", 'rb')
a = f.read(sizeof(BiosParameterBlock))
f.close()

BPB = cast(a, POINTER(BiosParameterBlock) ).contents

RootDirSectors = ((BPB.BPB_RootEncCnt * 32) + (BPB.BPB_BytsPerSec - 1)) //
BPB_BPB_BytsPerSec

FATSz = BPB.BPB_FATSz32

BytesPerSector = BPB.BPB_BytsPerSec

FirstDataSector = BPB.BPB_ResvdSecCnt + (BPB.BPB_NumFATs + FATSz) + RootDirSectors

OffsetDataDir = BytesPerSector * FirstDataSector
```

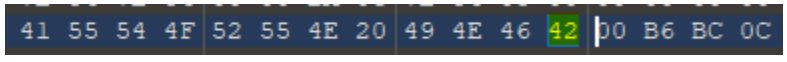
OffsetDataDir = 4194304 (0x400000)
Bundan sonra hexa editor ilə həmin offsetə getdim.



Burada ki, 32 baytlıq məlumatların strukturu aşağıdaki kimidir. Burada bizə lazım olan **Attribute** dəyəridir.

Offset in the Entry	Length in Bytes	Description
00	8	Filename
08	3	Extension
0B	1	Attribute
0C	1	Case
0D	1	Creation time in ms
0E	2	Creation time
10	2	Creation date
12	2	Last access date
14	2	High word of starting cluster for FAT32
16	2	Time stamp
18	2	Date stamp
1A	2	Starting cluster
1C	4	Size of the file

Cari diskdə autorun.inf faylı üçün bu dəyər **0x42** idi. Bu isə file attribute tablosunda **ATTR_HIDDEN** dəyərinə qarşılıq gəlirdi.



Value	*Meaning*
01	Read Only
02	Hidden
04	System
08	Volume Label
10	Directory
20	Archive
40	Unused
80	Unused

Nəticə:

USB Vaccine proqram təminatı diskə yazdığı Autorun.inf faylının atrributunu **HIDDEN** verdiyi üçün fayla access ala bilmirdim. Test etmək üçün faylın attributunu "0" olaraq dəyişdim və faylı yenidən silməyə cəhd etdim. *Fayl uğurla silindi.*

İstinadlar

https://www.pandasecurity.com/en/mediacenter/products/panda-usb-and-autorun-vaccine/
https://en.wikipedia.org/wiki/File_Allocation_Table
https://download.microsoft.com/download/1/6/1/161ba512-40e2-4cc9-843a-923143f3456c/fatgen103.doc
https://averstak.tripod.com/fatdox/dir.htm