ANDROMEDA-(AVALANCHE)

Avalanche, Avalanche-Andromeda, болон Andromeda хортой программууд нь кибер гэмт хэрэгтнүүдийн өргөн ашигладаг botnet, хортой программын нэг төрлүүд бөгөөд тэдгээр нь дэлхийн олон улсад тархаж, томоохон хэмжээний хохирол учруулж байсан.

AVALANCHE

Avalanche бол кибер гэмт хэрэгтнүүдийн үйл ажиллагааг дэмжих томоохон ботнет платформ байсан бөгөөд 2009 оноос 2016 онд буулт хийх хүртлээ олон төрлийн хортой программын тархаах, хяналт удирдлагаа явуулж байсан.

Avalache нь өөрөө хортой код бус харин malware hosting network буюу хортой кодуудыг өөр дээрээ хадгалах, тараах үйлдэл хийдэг өөрийн дэд бүтэцтэй хоорондоо холбоотой серверүүд юм

Avalanche платформын онцлог:

- Олон төрлийн хортой программ тараах: Avalanche нь банкны мэдээлэл хулгайлах, ransomware, фишинг халдлагууд, мөн бусад төрлийн хортой программ тараахад ашиглагддаг байсан.
- Хортой программыг тархаах дэд бүтэц: Avalanche нь дэлхийн олон улс дахь ботнетүүдийг ашиглан спам мэйл илгээх, хуурамч вэбсайтад хэрэглэгчдийг оруулах, банкны картын мэдээлэл хулгайлах гэх мэт олон төрлийн кибер халдлагыг зохион байгуулж байсан.
- DNS Fast-Flux техник ашигласан: Avalanche платформ нь DNS fast-flux техникийг ашиглаж байсан. Энэ нь серверүүдийн байршил болон IP хаягийг байнга өөрчлөх замаар хортой программын команд хяналтын серверийг илрэхээс хамгаалдаг.

Avalanche-ийн гол аюул:

- Фишинг кампанит ажил: Кибер гэмт хэрэгтнүүд фишинг мэйл илгээж, хэрэглэгчдийг хуурамч вэбсайт руу хөтөлж, хувийн мэдээлэл, банкны мэдээллийг нь хулгайлдаг байв.
- Ransomware тархаах: Avalanche-ээр дамжуулан ransomware программуудын олон төрлийг тарааж байсан бөгөөд хэрэглэгчдийн файлуудыг шифрлэж мөнгө нэхдэг байв.

Avalanche-ийн зогсолт:

- 2016 онд олон улсын хууль сахиулах байгууллагуудын хамтын ажиллагааны үр дүнд Avalanche сүлжээг тасалдуулж, түүний команд-хяналтын серверүүдийг хаасан. Гэсэн хэдий ч уг платформын хортой үр дагавар удаан хугацаанд үлдсэн.

ANDROMEDA

Andromeda бол олон төрлийн хортой программ тархаах, системүүдийг халдварлуулж удирдах ботнет хөтөлбөр юм. Энэ нь голчлон банкны мэдээлэл хулгайлах болон өөр хортой программ суулгахад ашиглагдаж байсан.

Andromeda-ийн онцлог:

- Хууль бус программуудыг татах: Andromeda нь хэрэглэгчдийг хортой программ агуулсан хууль бус программ татах линкнүүдэд дарахыг өдөөнө.
- Модулиудын уян хатан байдал: Andromeda нь олон төрлийн үйлдэл гүйцэтгэх боломжтой модулиудаас бүрдэнэ. Жишээ нь, хэрэглэгчийн нэр нууц үг хулгайлах, хуурамч программ суулгах, болон системд нэвтрэх замыг нээх зэрэг үүрэгтэй.
- Бүх төрлийн хортой программ суулгах: Энэ хортой программ нь халдварласан системд банкны Trojan, ransomware, фишинг хэрэгслүүдийг суулгаж, бусад кибер гэмт хэрэгтнүүдэд системийг ашиглах боломж олгодог байсан.

Andromeda-ийн нөлөө:

- Олон төрлийн хортой программ тараах: Andromeda нь өөрийгөө тарааж, ботнетийн шинэ системүүдэд нэвтрэн орж байсан. Үүнээс гадна ransomware, банкны хортой программ, болон мэдээлэл хулгайлах хэрэгслүүдийг тараадаг байв.

Andromeda-ийн тасалдалт:

- 2017 онд Andromeda ботнетийг олон улсын хамтын ажиллагааны үр дүнд буулгаж чадсан. Европын Холбооны Кибер Аюулгүй Байдлын Агентлаг (ENISA), АНУ-ын FBI зэрэг байгууллагууд энэ ажиллагаанд оролцсон бөгөөд команд-хяналтын серверүүдийг тасалдуулсан юм.

ANDROMEDA ХОРТОЙ КОДЫГ ГАРААР УСТГАХ АРГА:

Халдлагын индикаторт (IoC) дурдагдсан өөрчлөлтүүдийг буцаан хийснээр Andromeda хортой кодыг компьютероос устгах боломжтой.

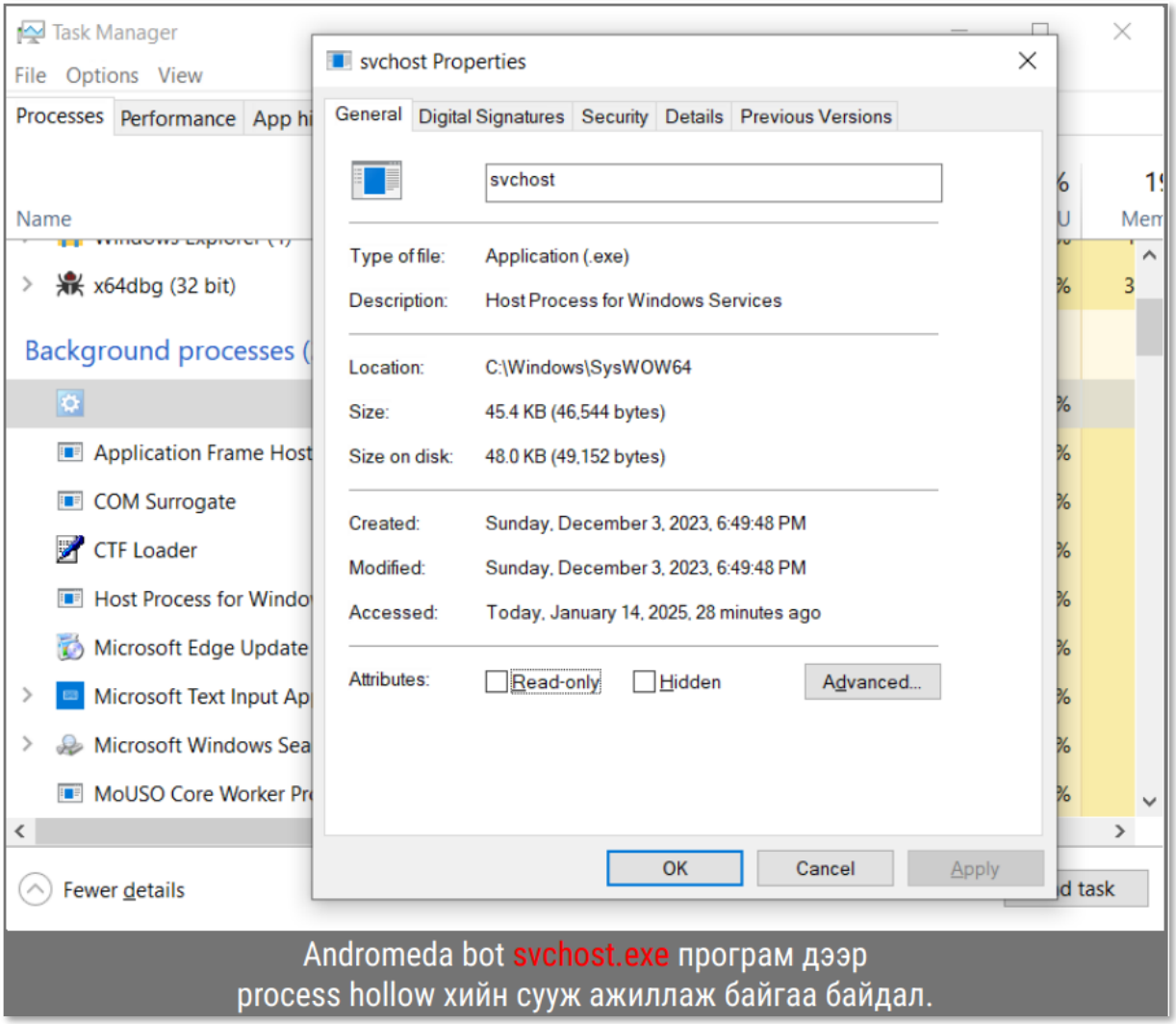
Гар аргаар устгахын тулд дараах алхмуудыг хийнэ:

АЛХАМ №1: Ажиллаж буй программын жагсаалт дундаас хортой кодыг олно. Andromeda хортой код нь хувилбараас болон үйлдлийн системийн архитектураас (x86 буюу x64) хамаарч

- C:\Windows\System32 (буюу SysWow64)\svchost.exe,
- C:\Windows\System32 (буюу SysWow64)\wuauclt.exe эсвэл
- C:\Windows\System32 (буюу SysWow64)\msiexec.exe программуудын оронд суудаг тул дээрх нэртэй программуудыг олно. Программын нэрийг шалгахдаа сэжигтэй процесс дээр баруун дарж properties сонгон зам болон программын нэрийг харж болно.

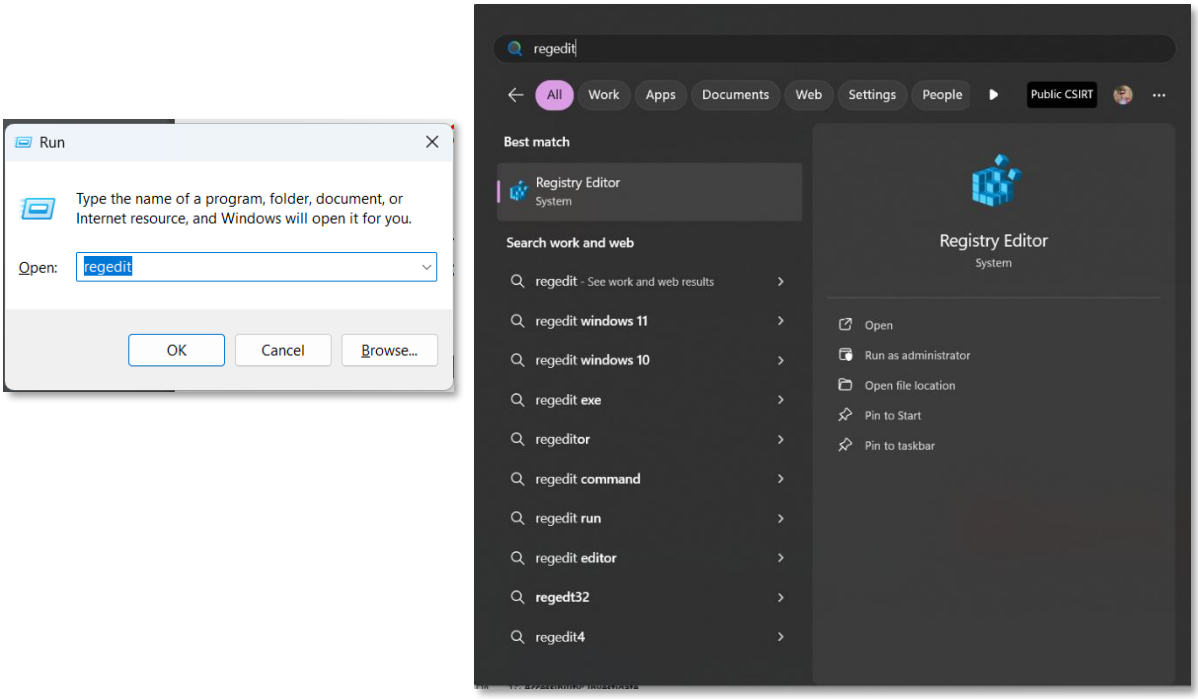
АНХААРАХ ЗҮЙЛС:

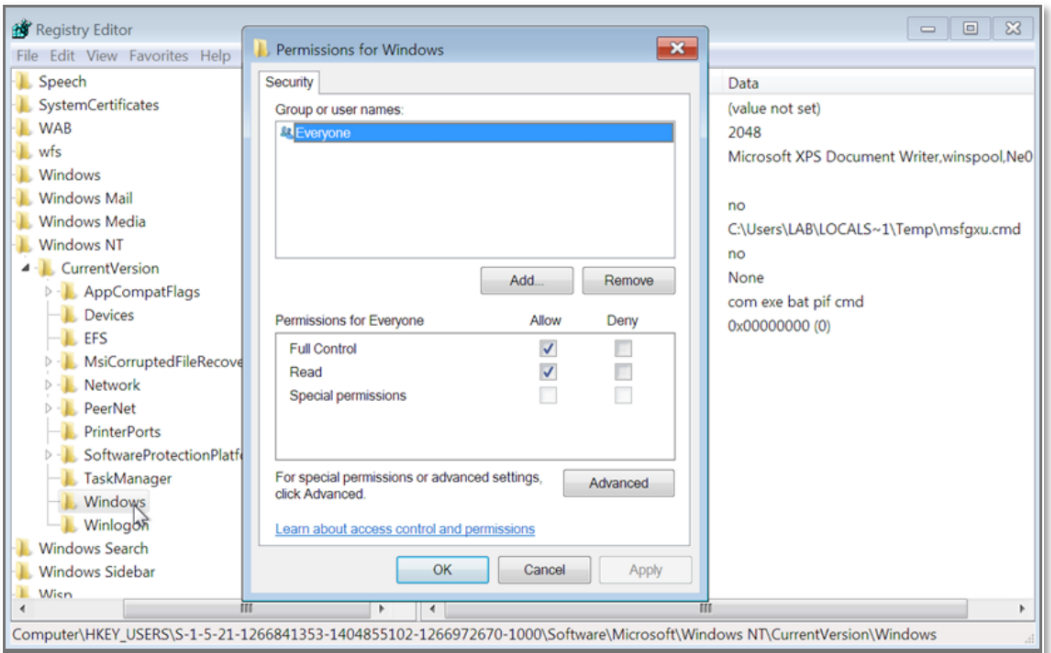
- Дээрх программууд нь үйлдлийн системийн бүрэлдэхүүн хэсэг тул хортой кодын хажуугаар давхар ажиллаж байх боломжтой тул зөвхөн нэрээр танихаас гадна файлын хэмжээ гэх мэт бусад индикаторуудыг харна (Andromeda хортой код нь 15-40 килобайт хэмжээтэй).
- svchost.exe программ нь жагсаалт дотор нэргүй харагдана (хавсаргасан зураг харна уу) Олдсон процессыг “End process” сонгон хаана.



АЛХАМ №2: Start цэсээс “Regedit” сонгох буюу өгөгдлийн сангийн жагсаалт руу орж үйлдлийн системээс хамаарч доорх 2 утгын аль нэгийг устгана:

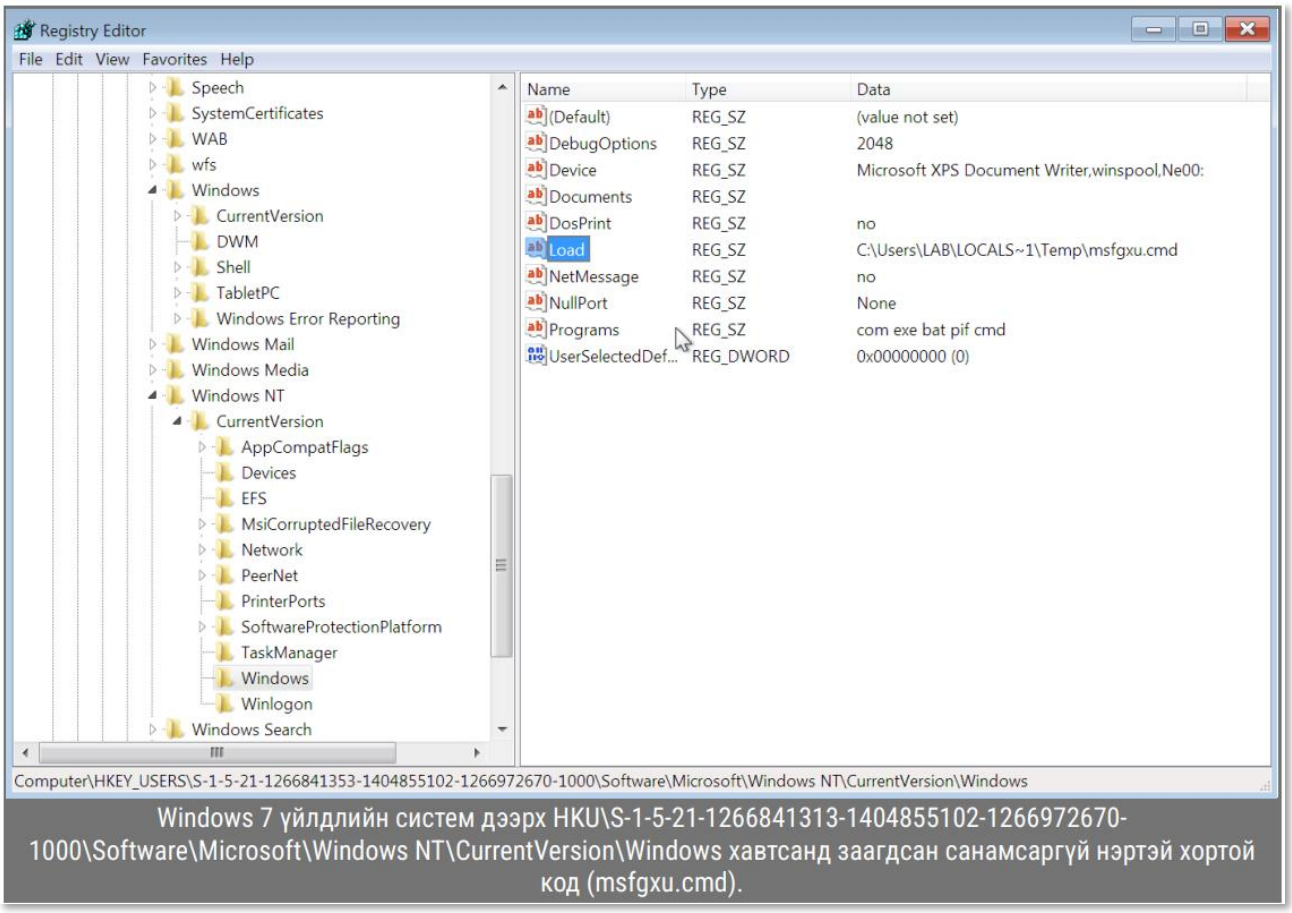
- HKU\S-1-5-21-1266841313-1404855102-1266972670-100016\Software\Microsoft\Windows NT\CurrentVersion\Windows\. эсвэл
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\64153: "C:\PROGRA~3\LOCALS~1\Temp\."





Windows 7 үйлдлийн систем дээрх HKU\S-1-5-21-1266841313-1404855102-1266972670-1000\Software\Microsoft\Windows NT\CurrentVersion\Windows хавтасны өөрчлөх эрхийг засч буй байдал

Өөрчлөх эрх нэмсний дараагаар “Load” түлхүүрт буй утгыг хулганы баруун сонголтод буй “Delete” сонголтоор устгана:



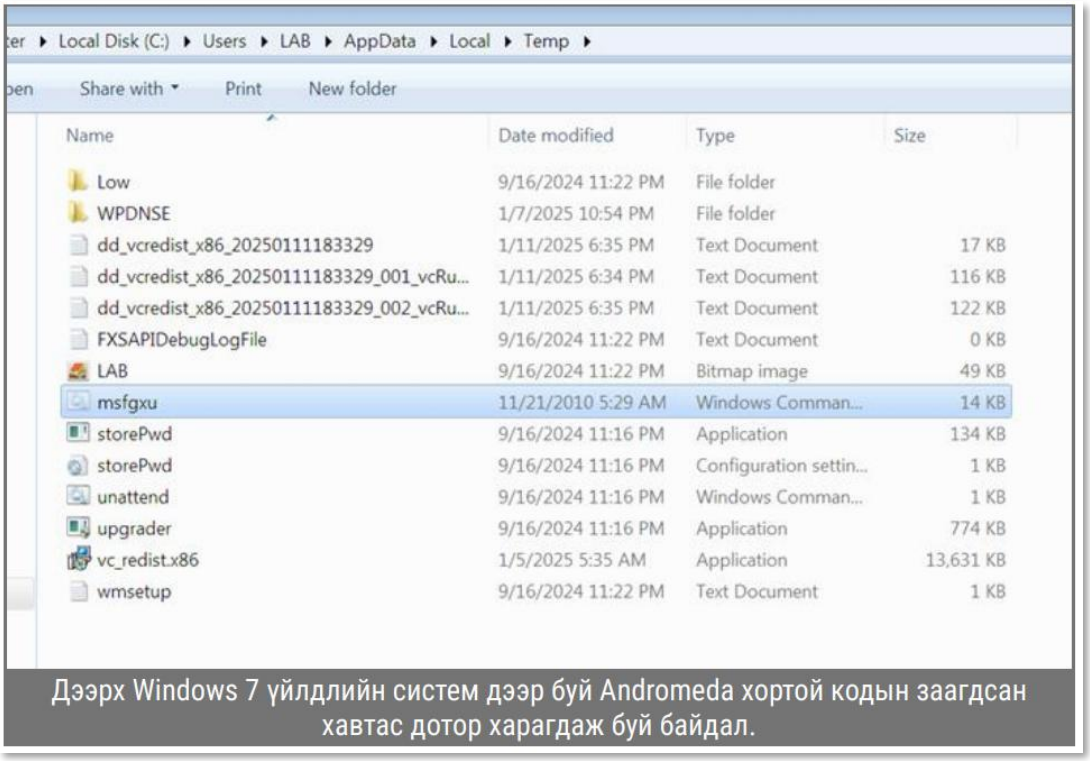
Windows 7 үйлдлийн систем дээрх HKU\S-1-5-21-1266841313-1404855102-1266972670-1000\Software\Microsoft\Windows NT\CurrentVersion\Windows хавтсанд заагдсан санамсаргүй нэртэй хортой код (msfgxu.cmd).

АНХААРАХ ЗҮЙЛС:

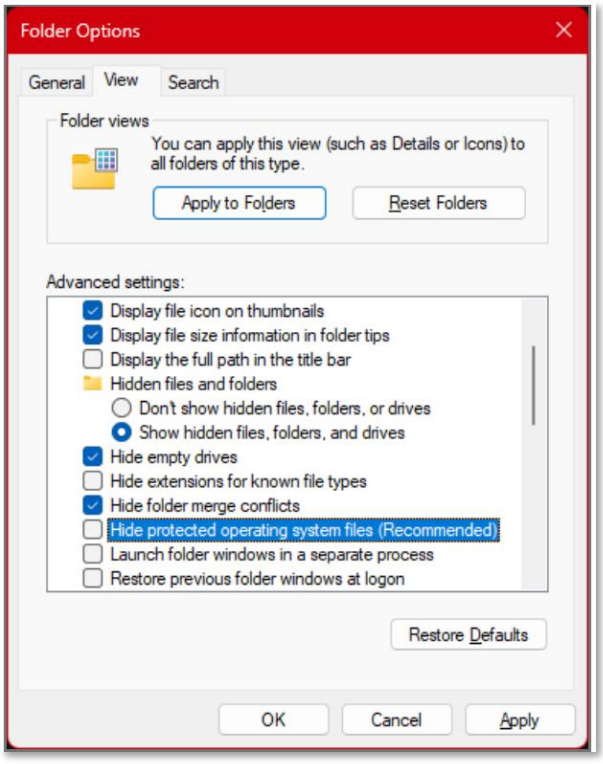
- Andromeda хортой код нь өөрийгөө хуулахдаа санамсаргүй утга сонгодог тул нэр ямар ч байж болохыг анхаарна уу.
- Хортой код нь өөрчилсөн буюу нэмсэн өгөгдлөө хэрэглэгч өөрчлөх эрхгүйгээр нэмдэг тул тухайн санг агуулж буй хавтсанд хэрэглэгч өөрчлөх эрх нэмэх шаардлагатай. Нэмэхийн тулд агуулж буй хавтсан дээр хулганын баруун товч дарж “permission” сонголт руу орж “Full Control” болон “Read” эрхүүдийг чагтална (хавсралт зураг харна уу).

АЛХАМ №3: Тухайн өгөгдлийн сан дээр нэмэгдсэн байсан хэсэг рүү орж тухайн хортой кодын файлыг устгана. Зам нь ихэвчлэн:

- C:\ProgramData\Local Settings\Temp\ эсвэл
- C:\Users\\AppData\Local\Temp\ байна.



АНХААРАХ ЗҮЙЛС: Temp хавтас болон хортой кодын программ нь систем файлын нууцлалтай байдаг тул файл хандагч программуудад (Windows explorer) харагдахгүй байх боломжтойг анхаарна уу. Харагддаг болгохын тулд Folder Options – View хэсэг рүү орж "Show Hidden Files, …" сонголтыг сонгож, "Hide Protected Operating System Files" чагтыг арилгана:



Дээрх үйлдлүүдийг буюу алхам №1, №2, №3 хийсний дараагаар **компьютерыг унтрааж асаан, ажиллаж буй программын дунд байхгүй болсон эсэхийг** нягтална.

АНХААРАХ ЗҮЙЛ: Andromeda хортой код нь өөр хортой кодыг татаж ажиллуулах үндсэн үүрэгтэй тул түүгээр нь дамжин өөр хортой код мэдэгдэлгүй халдварласан байх магадлал өндөртэй тул антивирусын программаар компьютероо бүрэн шалгах нь зайлшгүй шаардлагатайг анхааараарай.