

Creative Commons Attribution-ShareAlike 4.0 International License (CC BY-SA 4.0)

Ish nomi: Malware-Prevention-Method

Muallif: Anvar Kutlimuratov

Yaratilgan yili: 2009

Ishning to'liq tavsifi

1. Kirish

Zamonaviy zararli dasturlar (malware) tobora murakkablashib bormoqda va an'anaviy antivirus tizimlari har doim ham ularga qarshi samarali himoya bera olmaydi. Ushbu hujjatda taklif etilayotgan **Malware-Prevention-Method** usuli **fayl kengaytmalarini o'zgartirish orqali zararli dasturlarni tizimda ishlashiga yo'l qo'ymaslik** g'oyasiga asoslangan. Ushbu metod **an'anaviy antiviruslarga muqobil yondashuv** sifatida ishlab chiqilgan va 2009-yildan buyon amaliy sinovdan o'tkazilgan.

2. Ishlash prinsipi

Ushbu usul quyidagi tamoyillar asosida ishlaydi:

1. **Fayl kengaytmalarini o'zgartirish** – Windows operatsion tizimidagi bajariluvchi fayllarning kengaytmalarini standart .exe formatidan o'zgartirib, masalan, .123 formatiga o'tkazish.
2. **Tizim darajasida bajarilishni oldini olish** – Zararli dasturlar odatda .exe formatida tarqaladi. Agar tizim .exe kengaytmali fayllarni ishlatishni tanimasa, virus o'z-o'zidan ishga tushmaydi.
3. **Faoliyat monitoringi** – Agar zararli dastur o'z-o'zidan .exe formatini qayta tiklamoqchi bo'lsa, tizim uni tanimaydi va ishlata olmaydi.
4. **Foydalanuvchi tomonidan boshqarish** – Faqat ishonchli dasturlar yangi formatda (.123) ishga tushirilishi mumkin.

3. An'anaviy usullardan farqi

An'anaviy antivirus dasturlari zararli dasturlarni quyidagi usullarda aniqlaydi:

- **Imzo asosida aniqlash (Signature-based detection)** – Oldindan ma'lum virus imzolari yordamida.
- **Xulq-atvor tahlili (Behavior-based analysis)** – Dastur ishlashi davomida shubhali harakatlarni aniqlash orqali.
- **Sandbox texnologiyasi** – Shubhali fayllarni alohida muhitda sinash orqali.

Ushbu usul esa **butunlay yangi yondashuvni taklif etadi**, chunki u zararli dasturlarni **aniqlashga urinmaydi, balki ularning ishlashiga yo'l qo'ymaydi**.

4. Tutilmaydigan yangi viruslarni qo'lga tushirish imkoniyati

An'anaviy antivirus tizimlari **zero-day** hujumlar yoki **o'zgaruvchan (polymorphic) viruslarni** aniqlashda qiynalishi mumkin. **Malware-Prevention-Method** esa bunday viruslarning o'zini oshkor qilishiga sabab bo'ladi, chunki ular bajarilish uchun **.exe** kengaytmasidan foydalanadi. Agar virus o'z-o'zini qayta tiklashga urinib, **.exe** formatini tiklamoqchi bo'lsa, tizim darhol foydalanuvchidan ushbu faylni qanday ochish kerakligini so'raydi. Bu esa foydalanuvchiga **shu zahotiyoq shubhali faoliyatni aniqlash va oldini olish** imkonini beradi.

Ushbu yondashuv **yangi va noma'lum viruslarni oldindan aniqlash** uchun kuchli vosita bo'lishi mumkin, chunki u har qanday zararli dasturlar uchun universal to'siq yaratadi.

5. Amaliy qo'llanilishi

Bu usul quyidagi sohalarda qo'llanilishi mumkin:

- **Korporativ IT xavfsizlik** – Kompaniyalarning ichki tarmog'ini zararli dasturlardan himoya qilish uchun.
- **Shaxsiy kompyuter foydalanuvchilari** – Oddiy foydalanuvchilar o'z kompyuterlarini qo'shimcha himoya qilishlari mumkin.
- **Bulutli xizmatlar va serverlar** – Serverlarni zararli dasturlar ta'siridan himoya qilish uchun.

6. Litsenziya haqida

Bu ish **Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0)** litsenziyasi asosida taqdim etiladi.

<https://creativecommons.org/licenses/by-sa/4.0/deed.uz>