MITSUBISHI ELECTRIC

MITSUBISHI CNC

Harici Hafıza Kartları Kullanma Talimatı

External Memory Usage Instruction (USB-CF)

M600, M700, PC

Hazırlayan

Erhan MALKOÇ
Mart 2009

GTS GENEL TEKNİK SİSTEMLER LTD. ŞTİ.

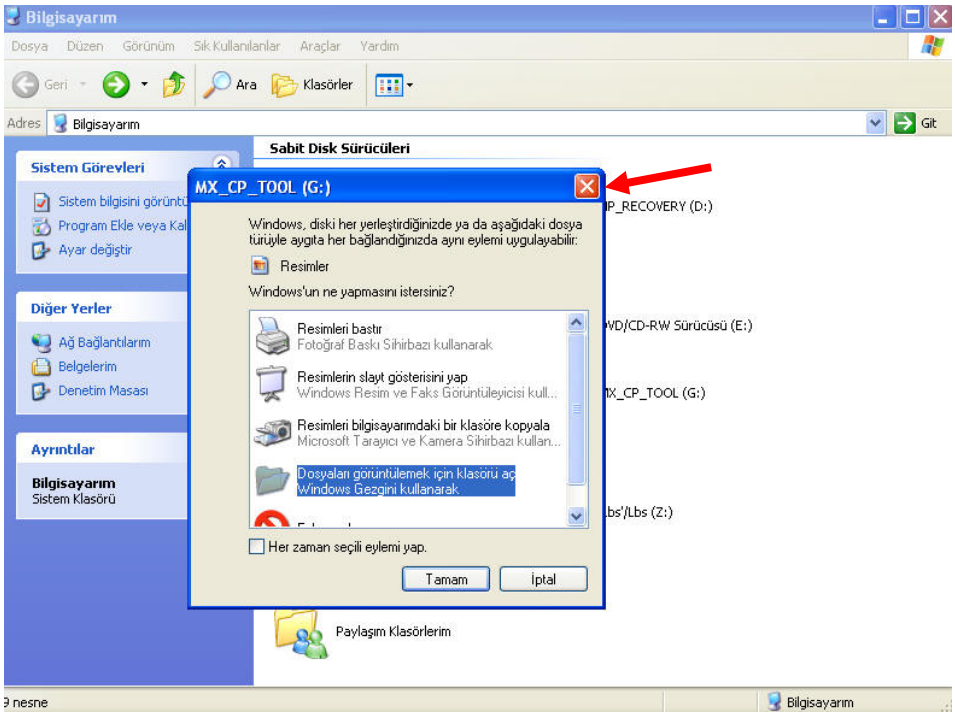
Günümüzde CNC makineler, endüstriyel makineler, robot sistemleri gibi bir çok sistemler PC tabanlı olarak üretilmekte ve kullanılmaktadır. PC tabanlı üretilen bu sistemlerde genelde Windows işletim sistemi yer almaktadır.
PC tabanlı sistemlerin kullanılmasıyla birlikte çeşitli bellek giriş çıkış üniteleri de bu sistemlerde kullanılmaktadır. Örneğin CF hafıza kartları, USB hafıza kartları gibi.
Mitsubishi CNC M600 ve M700 kontrol sistemleri de Windows işletim sistemi ile birlikte harici hafıza kartlarının kullanımına olanak veren sistemlerden biridir.
Kişisel bilgisayarlarımız da olduğu gibi kötü amaçlı yazılımlar ve virüsler makinelerimizi de tehdit edebilmektedirler.
Bu prosedürün amacı, herhangi bir sisteme takılan harici hafıza kartlarının kullanılması hakkında bilgi vermektir.

Harici Hafıza Kartlarında yaygın olarak bulunan kötü amaçlı yazılımların en dikkat çeken özelliklerinden biri bulaştığı sistemde gizli dosyaların gözükmesine engel olmaktır. Bu nedenle bu kartların içindeki kötü amaçlı yazılımlar da gizli olarak kayıtlı olduklarından, bir türlü bu tür kötü amaçlı yazılımları virüslü sistemlerde görüp silemeyiz.

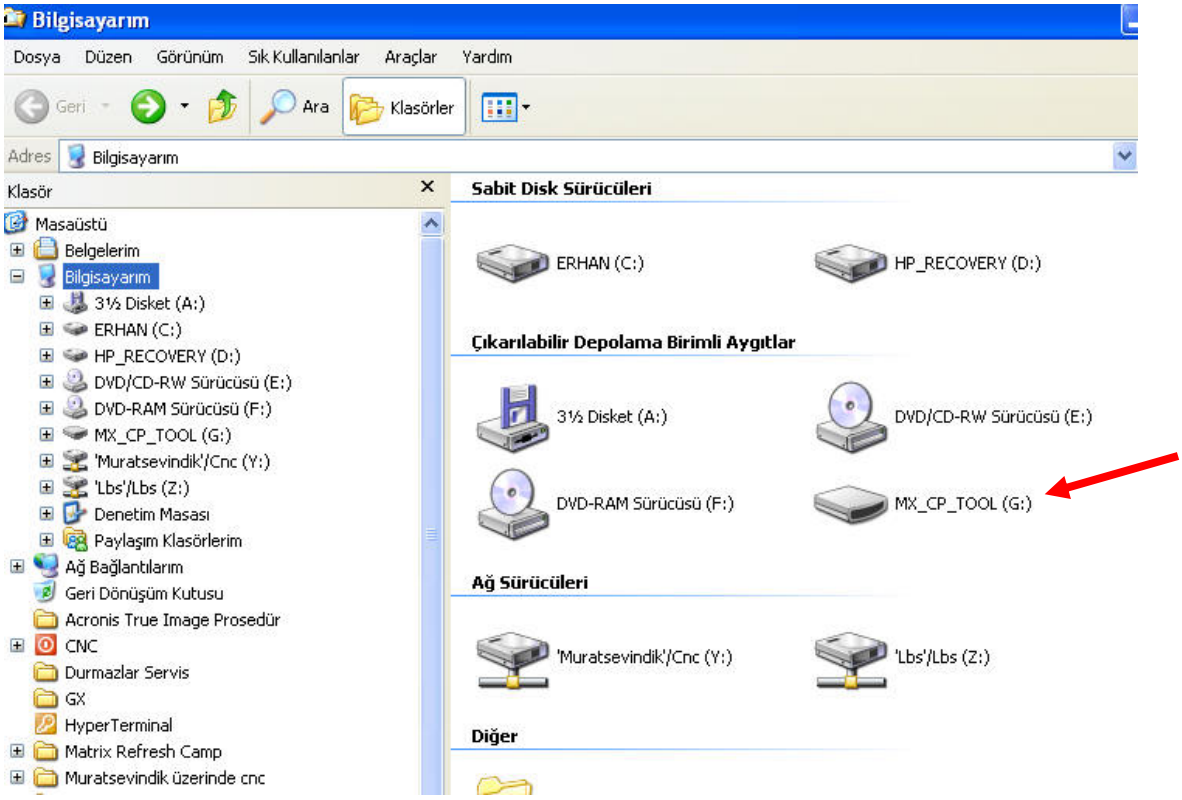
Harici Hafıza Kartlarında bulunan virüslerin bulaşma yöntemi nedir?

Harici Hafıza kartlarında bulunan virüsler genelde aynı tip bulaşma özelliği gösterirler. Temiz sistemlere takıldıkları zaman antivirüs programları genelde bu tür harici hafızalarını otomatik olarak taramazlar. Yada takılır takılmaz sadece belli başlı dosyalara bakıp (autorun.inf gibi) sadece bu dosyaları tarayıp silerler. Aslında bu sadece virüslerin yüklenmesini sağlayan ön dosyanın temizlenmesidir. Gerçek virüs dosyaları yine hafıza kartı içinde kayıtlı olarak durmaktadır.
Eğer bir harici hafıza kartı takılır takılmaz herhangi bir işlem yapılmaksızın manuel olarak kullanıcı tarafından herhangi bir virüs programı ile taratılırsa sorun ortadan kalkar. Fakat kişisel sistemlerimiz hariç makinelerde böyle bir şansımız bulunmamaktadır.
Herhangi bir harici hafıza kartı takıldığı zaman, Windows tarafından çıkan otomatik kullanımla içerik görüntülenirse veya Bilgisayarım içersinden bu hafıza kartı sürücü üzerine iki tıklayıp içerik görüntülenmek istenirse; hafıza kartı içersindeki kök dizinde bulunan autorun.inf dosyası otomatik olarak çalışır ve içersindeki kısayol kodları kullanılarak yine hafıza kartı içersindeki gerçek virüs dosyalarının çalıştırılmasına

imkan tanır. Böylece sistemimiz, antivirüs programları da yüklü olsa, kötü amaçlı yazılım tarafından ele geçirilir.



Şekilde görüldüğü gibi çıkacak otomatik kullanım penceresi mutlaka çarpı işaretinden kapatılıp kullanılmaması gerekir. Ayrıca aşağıda ki gibi G sürücüsüne kesinlikle 2 tıklayıp çalıştırılmaması gerekir. Bu virüslerin sisteme yüklenmesine neden olur.

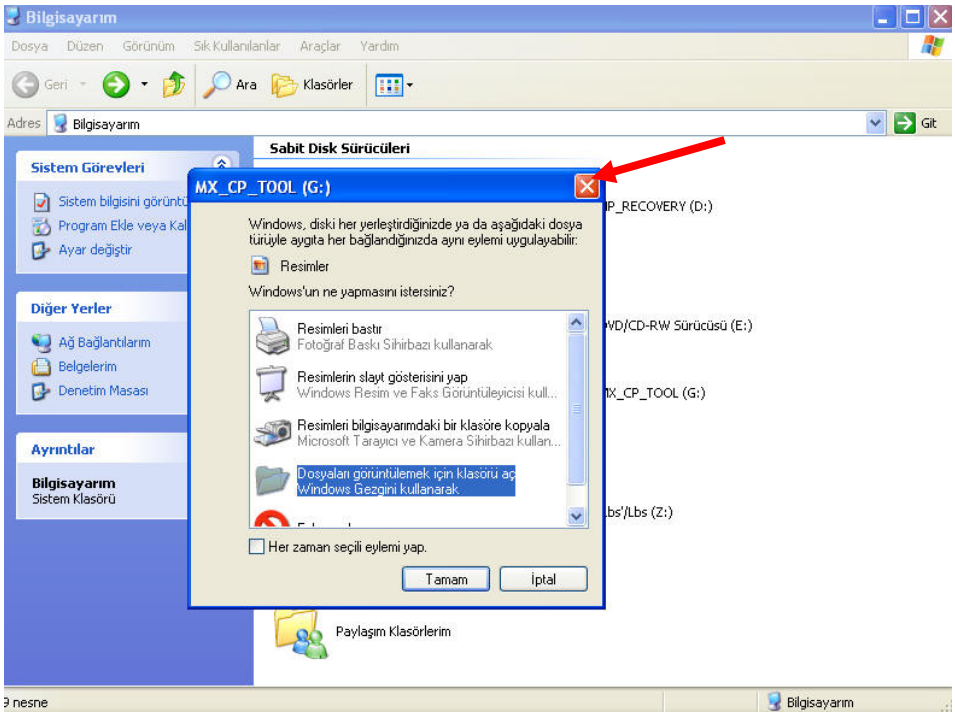


Unutmamak gerekir ki, eğer sistemimizde virüs varsa, hangi hafıza kartını takarsak takalım otomatik olarak virüs hafıza kartına yüklenecektir. Farkında olmadan bu hafıza kartını da başka sisteme virüs taşımada kullanabiliriz. Hafıza kartlarımızı korumak için yazma korumalı hafıza kartı kullanabilir veya virüslü sistemlere takmaktan kaçınabiliriz.

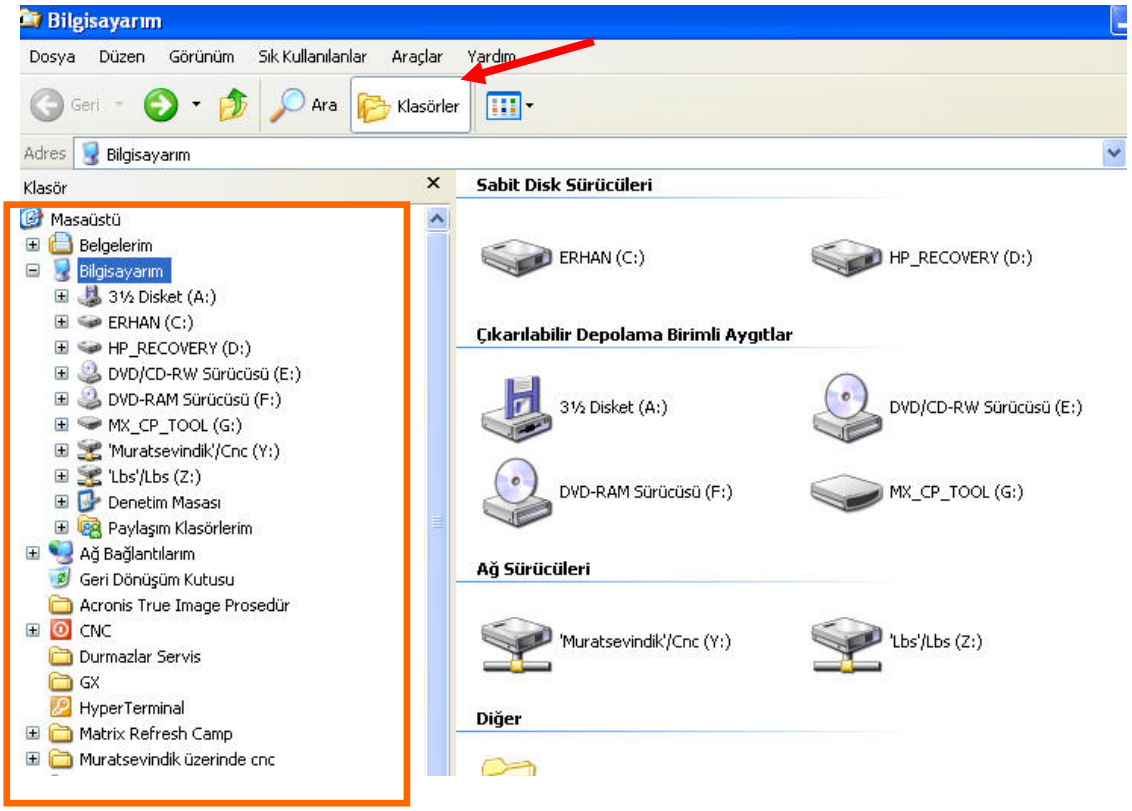
Eğer sistemimiz temiz bir sistem ise, harici hafıza kartımızda virüs olsa bile ve makinelerdeki gibi sistemimizde herhangi bir antivirüs programı yüklü olmasa bile, hafıza kartı içindeki virüsleri temizleyebilir ve işimizi halledebiliriz. Şimdi bunun yolunu sizlere göstermeye çalışacağız. Bu yöntemi her zaman kullanırsak taşıdığımız virüslerin yayılmasına engel olabiliriz.

Örneğin M700(MELDAS-MORI-MAZAK) kontrol sistemine sahip temiz bir sisteme USB bellek takıldığı zaman yapmamız gerekenler şunlardır.

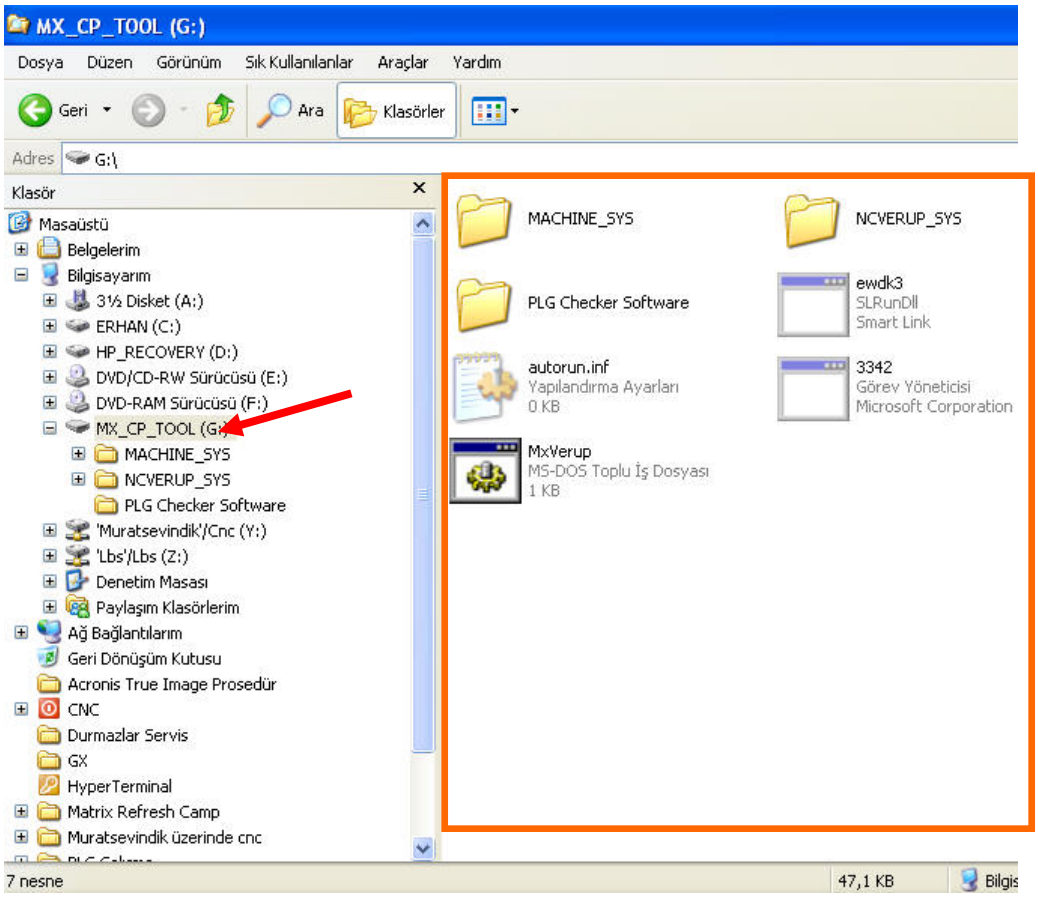
1. Öncelikle Windows otomatik çalıştır iptal edilecektir.



2. Kesinlikle harici bellek sürücüsü üzerine iki tıklanıp içerik görüntülenmeye çalışılmayacak bunun yerine üst menülerden klasörler tıklanacaktır. Bu sayede pencerenin sol tarafında sürücülerin listesini gösterir Windows gezgini penceresi açılacaktır.

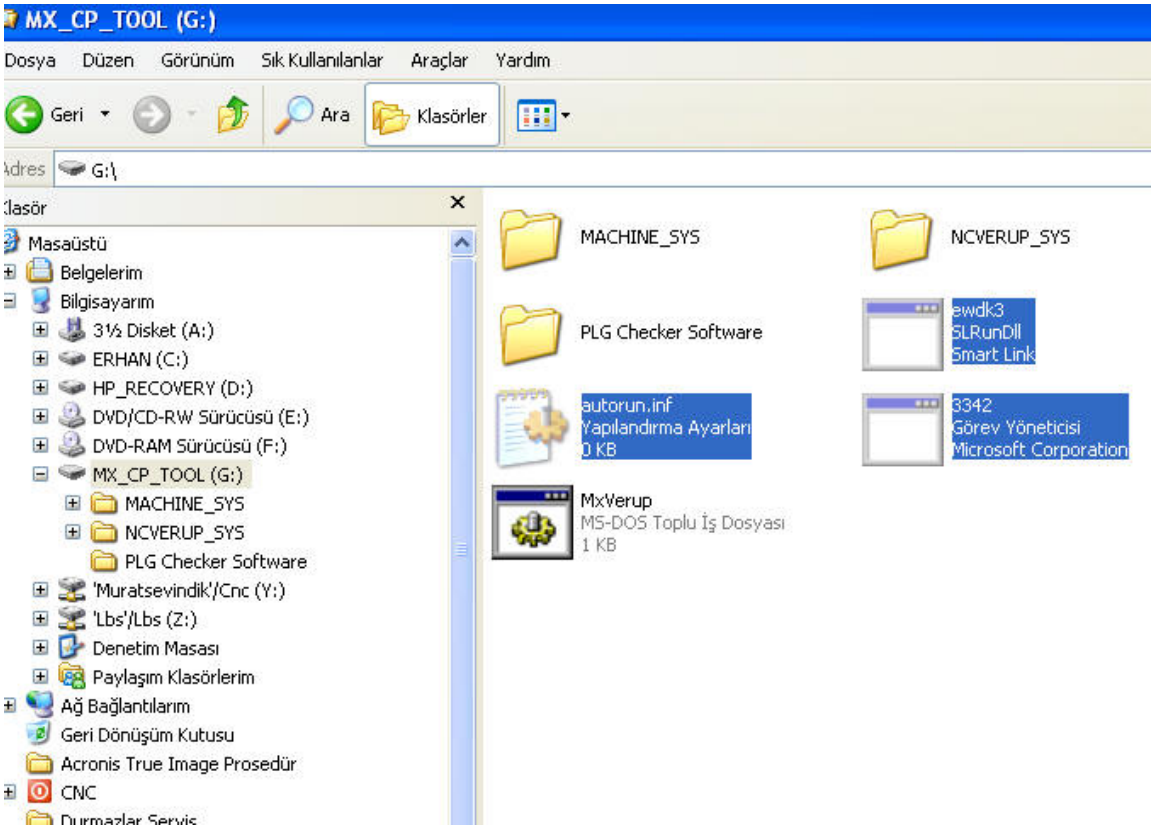


3. Bu gezgin penceresinden harici hafıza kartımız olan G sürücüsünün üzerine tıklanırsa G sürücüsünün içeriği sol taraftaki pencerede gözükecektir.



Yukarıdaki resimde de gözüktüğü üzere autorun.inf dosyası, ve çeşitli isimlerde 2 uygulama dosyası görmekteyiz. Bu dosyalar gizli dosya sınıfında olduğu için sistemimizde gizli dosyaları göster seçeneğinin açık olması gerekir.

Autorun inf dosyası otomatik çalıştır özelliğini kullanırsak ya da sürücü harfi üzerine direkt 2 tıklayarak çalışacak bir dosyadır ve içinde ki kodlarda virüs dosyaları olan 2 uygulama dosyasını çalıştıracak veriler vardır. Siz virüs dosyalarına doğrudan tıklayıp çalıştırmasanız bile bu dosyalar autorun.inf sayesinde çalışacak ve sisteminize bulaşacaktır.



Buradan sonra tek yapmamız gereken bu dosyaları seçmek ve doğrudan silmektir. Böylece hem USB hafızamız temizlenmiş olur hem de temiz olan makinemizin sistemine virüs bulaştırmamış oluruz.

Unutmayınız ki temizlemiş olduğunuz bu USB belleği yine virüs bulaşmış kişisel bilgisayarımıza taktığınız zaman bu virüsler otomatik olarak USB belleğinize geri yüklenecektir.

Virüslerden korunmanın tek ve geçerli yolu kendi kendimizi kontrol etmek ve bilinçli olmaktır. Çünkü tezgahlara virüs bulaştıranlar ve asıl sorumlu olanlar yine bizlerizdir.