STOP | THINK | CONNECT™

Botlar ve Botnetler

Genel Bilgiler & Öneriler

Bot ve Botnet nedir?

İnternetin insan hayatı için harika olanaklar sağladığı konusunda hiç şüphe yoktur; çünkü hem hayatımızı kolaylaştırmakta hem de bizleri dünyanın geri kalanına bağlamaktadır. Ne yazık ki, hayatı kolay hale getiren bu şeyi kontrol altına almak isteyen kötü niyetli insanlar bulunmaktadır. Yaygın siber suçların bir bölümü, bazı kötü amaçlı yazılım türleriyle, internete bağlı cihazlara bulaşarak, onları botlara (robotlara) dönüştürür.

Bir cihaz bir bot olduktan sonra, genellikle bir Botnet'in (robot ağı) parçası durumundadır. Botnet diğer tüm enfekte cihazların oluşturduğu büyük bir ağ olup, siber saldırganlar tarafından uzaktan kontrol edilir. Siber suçlular, bu botları istenmeyen e-postalar göndermek suretiyle maddi kazanç veya hırsızlık amacıyla daha fazla cihazı etkisi altına almak ya da sitelere saldırmak için kullanmaktadır. Bir botnet herhangi bir yerden yönetebildiği yüzlerce hatta binlerce cihaza sahip olabilmektedir

Ne Yapabiliriz?

Aşağıdaki öneriler ışığında hem kendimizi hem de başkalarını çeşitli kötü niyetli yazılımların saldırılarına karşı koruyabiliriz.

Makineniz Temiz Kalmalı

- En son çıkan ve en güncel güvenlik yazılımları, web tarayıcıları ve işletim sistemleri; virüsler, kötü amaçlı yazılımlar ve diğer çevrimiçi tehditlere karşı en iyi savunmadır.

Yedekleme

- Değerli çalışmaların, müziklerin, fotoğrafların ve diğer dijital bilgilerin düzenli bir şekilde elektronik kopyası oluşturulmalı ve güvenli bir şekilde saklanarak korunmalıdır.

Daha İyi Şifreler Oluşturma

- Güçlü bir parola bir cümleden oluşup en azından 12 karakter içermelidir. Şifre oluşturmak için hatırlaması kolay, beğenilen olumlu bir cümle veya deyimlere odaklanılmalıdır.

Şüpheye düştüğünüzde silin

- Siber suçlular genellikle e-postadaki bağlantılar, sosyal medya mesajları ve online reklamlar üzerinden kişisel bilgileri çalmaktadırlar. Kaynak biliniyor olsa bile, bir şey şüpheli göründüğünde derhal silinmelidir.

Bağla & Tarama Yap

- USB'ler ve diğer harici cihazlar virüsler veya farklı kötü amaçlı yazılımlarca enfekte olabilirler. Bu cihazları taramak için güvenlik yazılımları kullanılmalıdır.