Kanald.com.tr Hacklendi…

written by Mert SARICA | 22 Nisan, 2010

20:30 sıralarında http://www.kanald.com.tr sitesi bilgisayar korsanları tarafından hacklenerek sayfaya giren ziyaretçiler http://m3ng3nl1.by.ru/birand.html web sayfasına yönlendirildi. Her ne kadar korsanların sayfada yayınladıkları mesaj masum gibi görünsede aslında sayfanın kaynak kodu incelendiğinde heap-spray yöntemi ile yaması güncel olmayan Internet Explorer tarayıcısına sahip olan ziyaretçiler istismar edilmeye yani işletim sistemi ele geçirilmeye çalışılıyordu. İstismar kodunu kayıt edebildim, elimdeki verileri toparlamaya çalışıyorum, imkanım oldukça sizleri bilgilendireceğim. Internet Explorer sürümü güncel olmayanlarınız bu sayfayı ziyaret etti ise büyük tehlike altında olabilirsiniz bu nedenle işletim sisteminiz üzerindeki sıra dışı aktivitelere dikkat etmenizde fayda var…

Güncelleme @01:10: Benden bu kadar kendinizi ve ağınızı korumak istiyorsanız yapmanız gerekenler;

- 217.23.7.125 IP adresine doğru tüm trafiği yasaklayın ve izlemeye alın.
- xxx.exe adında işletim sisteminizde bir dosya varsa (MD5 hashi: b597c4a7451a84d94ff421f4ba3c4d6c) silin.
- windows\system32 klasörü altında a.exe adında bir dosya varsa (MD5 hashi: b597c4a7451a84d94ff421f4ba3c4d6c) silin.
- pcsecurity35@gmail.com e-posta adresine giden tüm e-postaları yasaklayın ve izlemeye alın.

Güncelleme @01:00: xxx.exe ve a.exe leetlogger adında bir tuş kayıt (keylogger) programı ve tuş kayıtlarını pcsecurity35@gmail.com e-posta adresine gönderiyor, dikkat!

Güncelleme @00:42: Istismar kodu http://217.23.7.125/xxx.exe dosyasını indirip çalıştırıyor ve daha sonra kendisini system32 klasörü altında a.exe adı altında saklıyor, dikkat!

Güncelleme @00:30: İstismar kodunun online analiz sonucu

Güncelleme @00:09: İstismar edilen güvenlik zafiyeti tespit edildi – MS10-018

Hedef IE sürümleri:

- Microsoft Internet Explorer 7, Windows Vista SP2
- Microsoft Internet Explorer 7, Windows XP SP3
- Microsoft Internet Explorer 6, Windows XP SP3

Güncelleme @22:01: Korsanlar kanald.com.tr sayfasının kaynak koduna aşağıdaki satırı eklemişler.

Korsanların yönlendirdiği sayfa:

Sayfanın IP adresi:

Host IPS alarmı:

Internet Explorer istismar kodu: