TÜBİMER
TÜBİTAK İLETİŞİM MERKEZİ

TÜBİTAK

GÖRÜŞ / ÖNERİ BAŞVURUSU

Başvuru Bilgileri

Başvuru Tarihi : 14.08.2022

Başvuru Numarası : 2208G1864

Başvuru Sahibi

TC Kimlik No	:	22733571022
Ad	:	SADIK KAAN
Soyad	:	GÜNDEM
E-Posta	:	magnetar07@hotmail.com
Telefon	:	0 505 668 07 99
İl	:	Antalya
İlçe	:	Muratpaşa
Posta Kodu	:	07042
Adres	:	Ücgen Mahallesi Tonguç Caddesi Bayram Duman Apartmanı 42/20 kat:6

Açıklama

Açıklama : Pardus işletim sistemi kullanıyorum. Bilgisayarım internete bağlı değilken bile format atmama, bios/uefi firmware yazılımını ve hard disk firmware yazılımını değiştirmiş olmama rağmen kendi kendine program açılıyor , fare imleci kendi kendine hareket ediyor ve bazen bilgisayar "sistemin öntanımlı ses servisi" kapalı şekilde açılmış oluyor. Wireshark programı ile incelediğimde usb portlarına takılı bir cihaz olmamasına rağmen usb portlarından interrupt sinyali geliyor. USB buslarından gelen interrupt sinyalleri linux'un boş
donanım olarak tanımladığı buslardan geliyor. Wireshark günlükleri

https://easyupload.io/eqrfr6 Bilgisayarımda NSA ANT COTTONMOUTH aracına benzeyen gizli bir usb implantı var. Bu implant bilgisayar açılışı sırasında linux veya windows işletim sistemi fark etmeksizin kernel'e aşırı yükleme yaparak kendisini gizli sistem processi olarak tanıtıp bütün antivirüs ve güvenlik yazılımlarını rahatça atlatabilir. Kernel güvenliğini aşamadığı bilgisayarlarda ise kendisini farklı bir donanım olarak tanıtıp aşırı interrupt yüklemesi yaparak bellek üzerinden sistemin kontrolünü ele geçiriyor. Bu durumu hiçbir antivirüs ve güvenlik yazılımı fark edemez. Anlayacağınız gibi bu gizli usb implantı ruber ducky ve usb ninja gibi basit bir "usb keyboard" değil kerneli ve sistem belleğini manipüle edebilen NSA COTTONMOUTH'a benzeyen gelişmiş bir usb casusluk implantıdır. Pardus ekibinden isteğim Pardus işletim sistem için gizli usb implantlarına karşı güvenlik modülü geliştirmeleridir.

Cevap Kanalı

Tercih Edilen Cevap Kanalı : Kısa mesaj
Sorumluluk metni'ni okudum ve kabul ediyorum : Evet