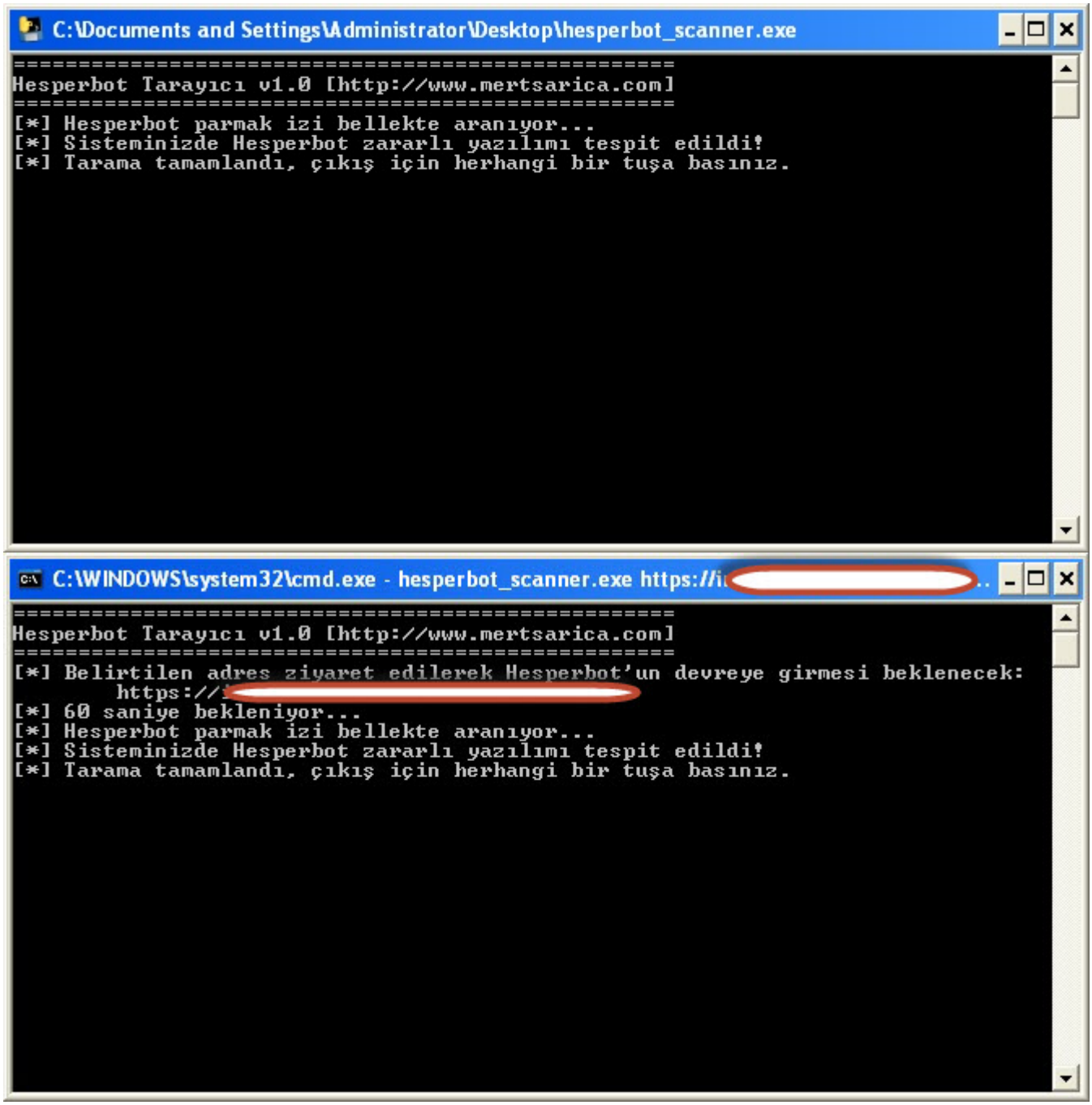
Hesperbot Tarayıcısı

written by Mert SARICA | 7 November 2014

Bildiğiniz gibi son 1.5 senedir vatandaşımız, Hesperbot adındaki ileri seviye internet bankacılığı zararlı yazılımı salgını (#1, #2, #3) ile boğuşmaktadır. Özellikle her yeni salgında siber dolandırıcıların, Hesperbot zararlı yazılımının imza tabanlı antivirüs ve benzer güvenlik yazılımları ve teknolojileri tarafından tespit edilememesi adına yapmış oldukları geliştirmeler ve buna ilaveten bu salgınlar ile ilgili olarak yazılı ve görsel medyada yapılan haberlerin sayıca yetersiz oluşu, her yeni salgında daha fazla vatandaşımızın mağdur olmasına sebebiyet vermektedir. Hesperbot üzerinde fazlasıyla mesai yapmış bir siber güvenlik uzmanı olarak, elde ettiğim bilgiler ışığında daha az vatandaşımızın mağdur olması adına sistem üzerinde Hesperbot zararlı yazılımının çalışıp çalışmadığını kontrol eden, Hesperbot Tarayıcısı adında basit ama etkili bir yardımcı araç hazırlamaya karar verdim. (Bu araç ayrıca siber güvenlik uzmanları, adli bilişim uzmanları, zararlı yazılım analistleri ve bilgisayar olayları müdahale ekipleri tarafından da kullanılabilir.)

Bu araç çalıştırıldığı anda bellek (RAM) üzerinde Hesperbot zararlı yazılımına ait parmak izi aramakta ve kullanıcıya tarama sonuna dair olumlu veya olumsuz bilgi vermektedir.

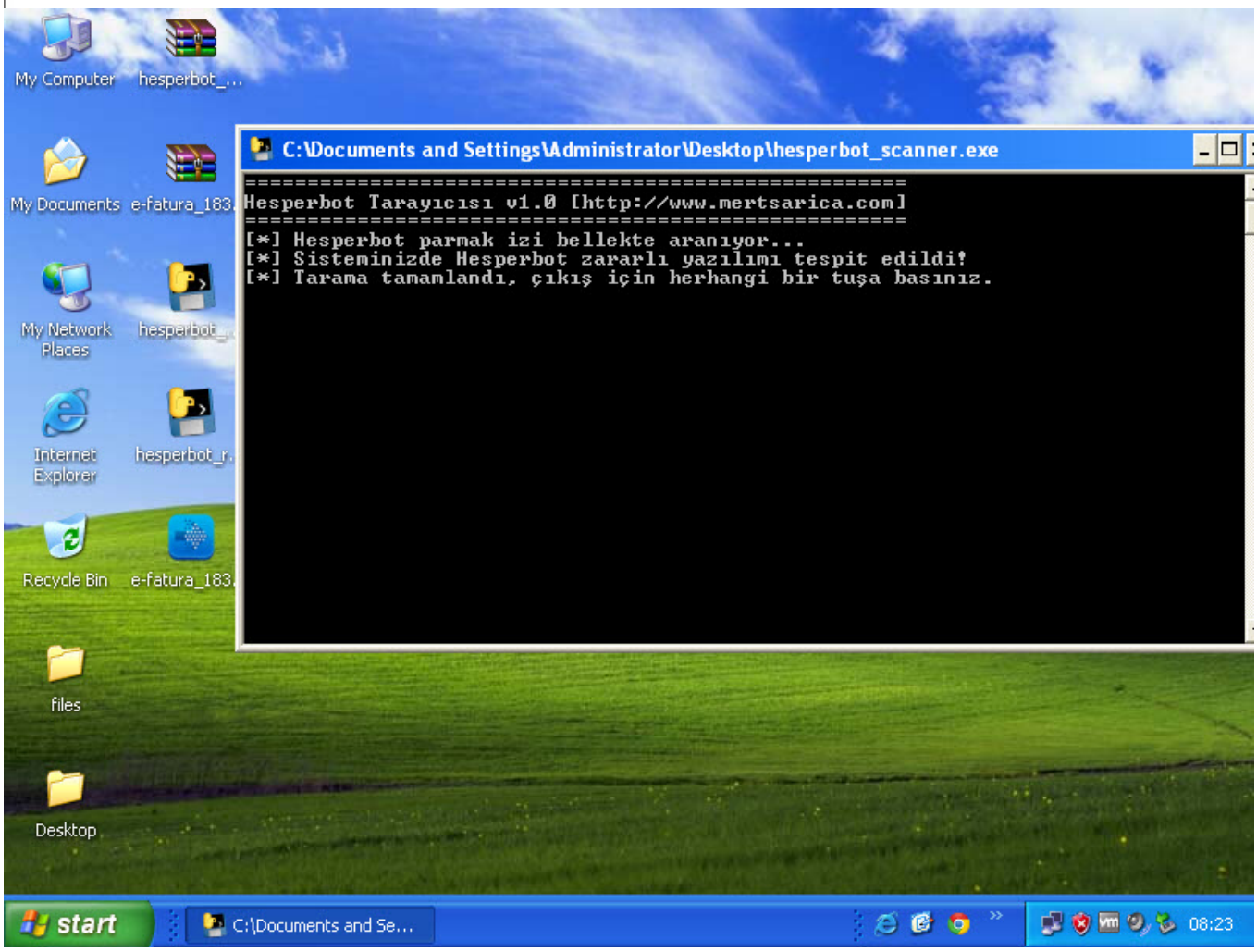
Aracı iki şekilde kullanabilirsiniz;
1. hesperbot_scanner.exe aracını Hesperbot zararlı yazılımının bulaştığından şüphe ettiğiniz sistem üzerinde çalıştırabilirsiniz.
2. hesperbot_scanner.exe [internet bankacılığı adresi] şeklinde çalıştırarak aracın belirttiğiniz bankanın internet bankacılığı web sayfasını otomatik olarak açmasını, Hesperbot devreye girene kadar bir dakika boyunca beklemesini (devreye girmeme ihtimaline karşı) ve ardından belleği taramasını sağlayabilirsiniz.



Hesperbot geliştiricilerinin ekmeğine yağ sürmemek için (biraz da onlar uğraşsınlar :)) kaynak kodunu paylaşmadığım Hesperbot Tarayıcısını buradan indirebilirsiniz.

Hesperbot Scanner aracı, 6 Kasım 2014 tarihinde başlayan Hesperbot salgınında gönderilen zararlı yazılım örneği üzerinde çalıştırılmış ve başarıyla Hesperbot bulaşmış sistemi tespit edebildiği teyit edilmiştir.

#	Result	Protocol	Host	URL
6	200	HTTP	Tunnel to	xseomagazine.ru:443
9	200	HTTPS	xseomagazine.ru	/g
10	200	HTTP	Tunnel to	xseomagazine.ru:443
11	200	HTTPS	xseomagazine.ru	/g
33	200	HTTP	Tunnel to	xseomagazine.ru:443
34	200	HTTPS	xseomagazine.ru	/g
35	200	HTTP	Tunnel to	tools.google.com:443
36	200	HTTP	Tunnel to	xseomagazine.ru:443
37	200	HTTPS	xseomagazine.ru	/g
38	200	HTTP	Tunnel to	xseomagazine.ru:443
39	200	HTTPS	xseomagazine.ru	/g
40	200	HTTP	Tunnel to	xseomagazine.ru:443
41	200	HTTPS	xseomagazine.ru	/g
42	200	HTTP	Tunnel to	xseomagazine.ru:443
43	200	HTTPS	xseomagazine.ru	/g



Aracın kullanımı için aşağıdaki videoyu aşağıdan izleyebilirsiniz.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

—- ENGLISH —-

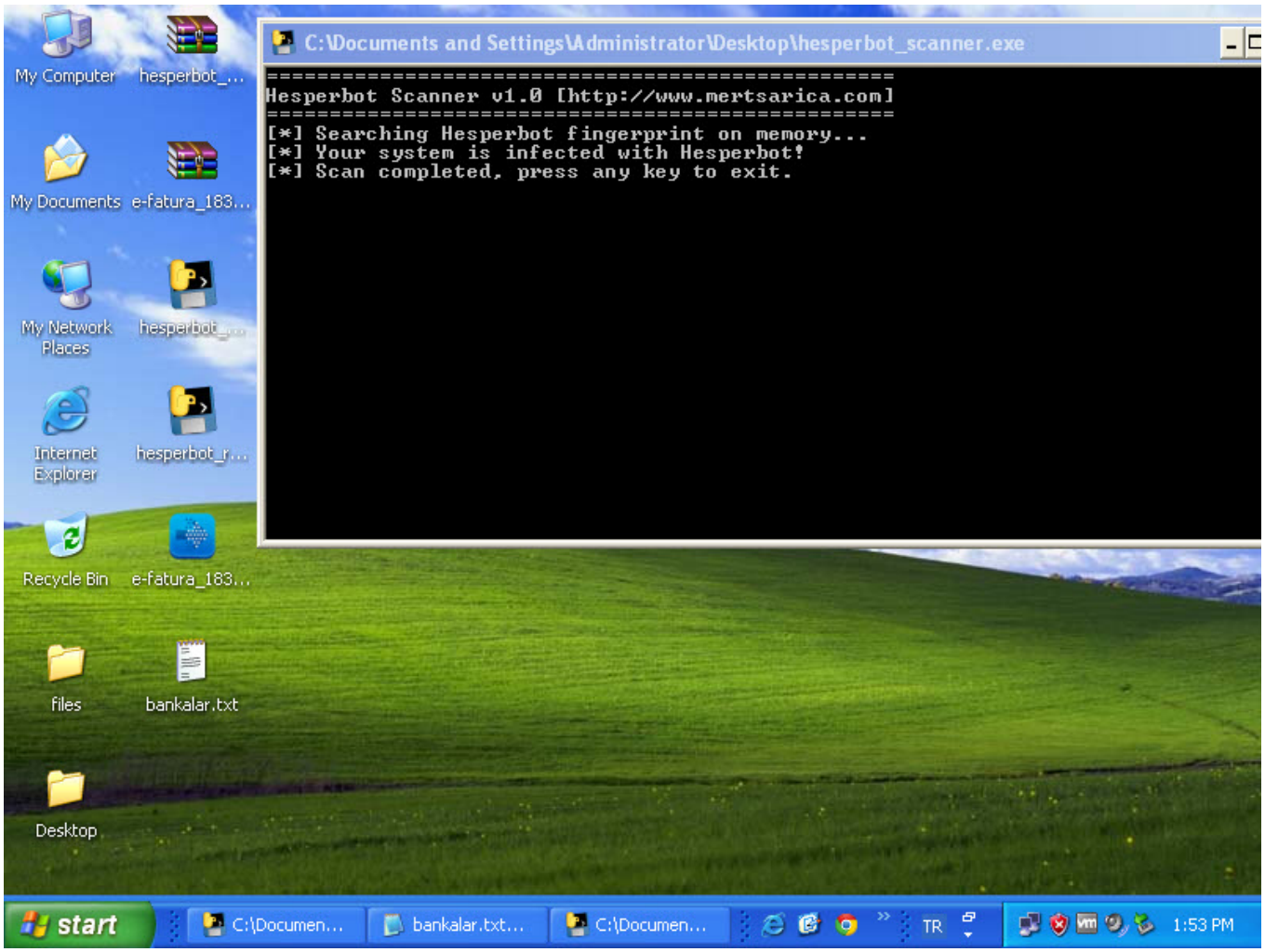
Hesperbot is an advanced internet banking trojan which is widespread (since 1.5 years) in Turkey. Hesperbot has keystroke logging, screenshots and video capture, hidden VNC server, network traffic interception and HTML injection

capabilities. (For more information, I suggest readers to take a look at Eset's great Hesperbot report.)

In every new Hesperbot campaign, bad guys release Hesperbot with new signatures therefore traditional security softwares/systems could not be able to detect it at the beginning of the campaigns so this situation forced me to code a tiny tool called Hesperbot Scanner. This tool is able to detect Hesperbot by searching memory for Hesperbot fingerprint. This tool is prepared for end users and for security professionals working in the information security, computer forensics, incident response and malware analysis fields.

Usage of Hesperbot Scanner is pretty simple, just run it on the infected/suspected system and check the result.

Click here to download Hesperbot Scanner



Regards,