Şeytan İkiz

written by Mert SARICA | 19 June 2011

Geçtiğimiz aylarda RSA'in sistemlerine sızan kişilerin Securid ile ilgili bilgileri çaldıkları ortaya çıktı. RSA tarafından yapılan açıklamada saldırıların başlangıç noktasında sosyal mühendislik ve olta saldırısı (phishing) olduğu dikkat çekiyordu. Olta saldırısını gerçekleştirmek için sosyal ağlardan faydalanan ahlaksız korsanların RSA çalışanlarına ait bilgileri elde ettikleri tahmin ediliyor.

İşin içinde insan faktörü olduğu sürece 100 haneli şifre ile korunan bir sisteme sızmak isteyenler, şifreyi kırmak yerine sistem sorumlularını kandırma yolunu tercih ediyorlar ve eninde sonunda başarıya ulaşıyorlar bu nedenle RSA'in başına gelenlere çok şaşırmıyorum özellikle sosyal ağlarda, firma çalışanları tarafından paylaşılan bilgilerin ilerleyen zamanlarda çoğu firmanın başını daha çok ağrıtacağını düşünüyorum.

Art niyetli kişiler, sosyal mühendislik saldırılarında olta saldırılarından faydalandıkları gibi şeytan ikiz (Türkçe mealini kendim uydurdum, aslı evil twin/kötü ikiz) yönteminden de faydalanabiliyorlar. Şeytan ikiz yöntemi, teknolojinin nimetlerinden faydalanarak hedef kurum/sistemler hakkında o kurumun bir çalışanını taklit ederek hedef kişi/kişiler üzerinden bilgi toplamak, kurum sistemlerine sızmak için hedef kişi/kişilerin zararlı bir dosyayı (RAT) çalıştırmaları amacıyla kullanılıyor.

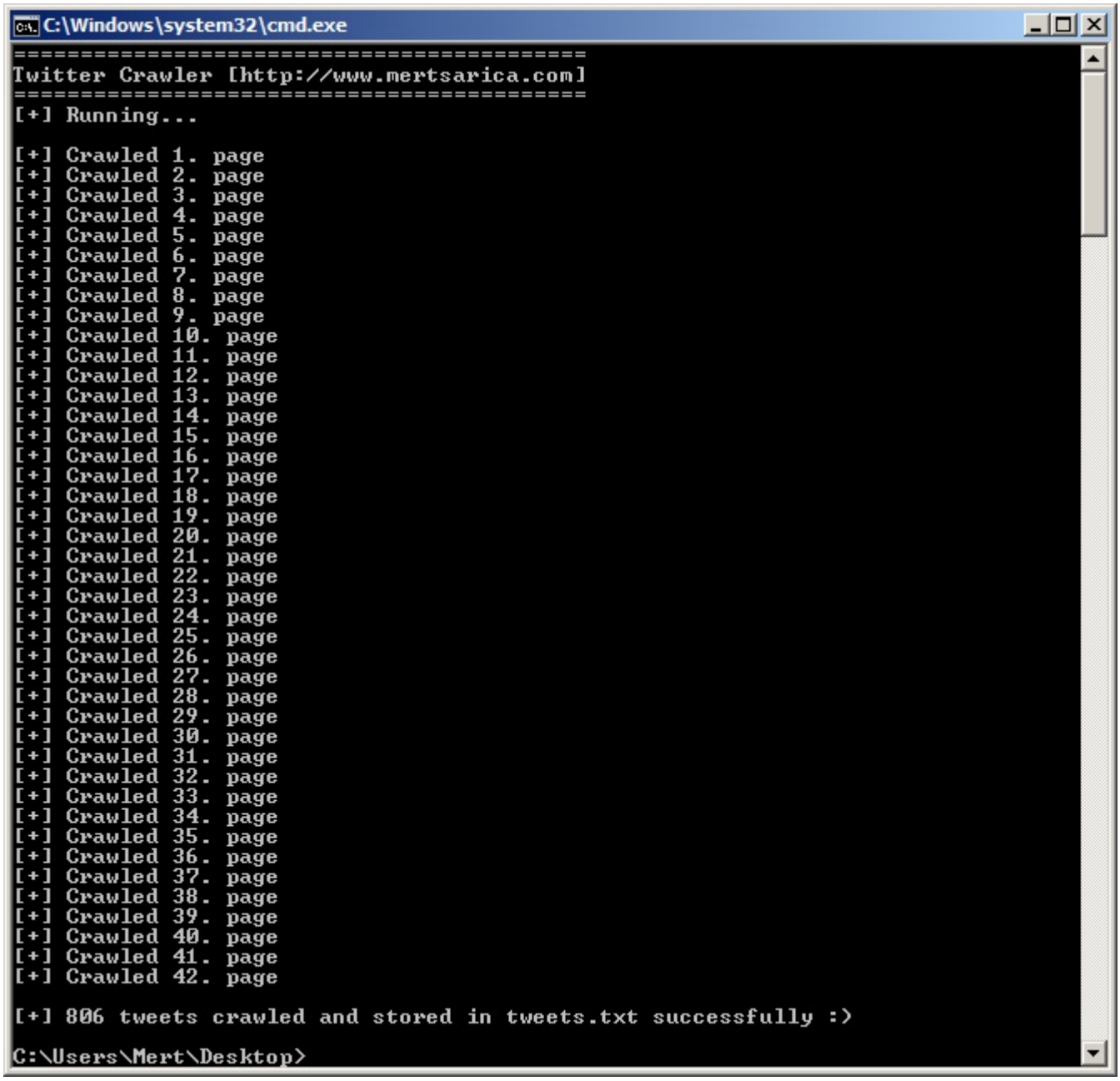
Amaçları gerçek bir kişiyi taklit etmek olduğu için art niyetli kişiler kurban ile ilgili tüm bilgileri Facebook, Twitter, Linkedin, Foursquare gibi sosyal ağlardan toplayarak bir araya getiriler. Facebook ve Twitter durum mesajları üzerinden bu kişinin neler yaptığını, Linkedin üzerinden özgeçmişini, Foursquare üzerinden hangi mekanlara sıkça uğradığını, Google arama motoru üzerinden de elde edebildikleri geri kalan bilgileri elde ederek hedef bir sosyal ağ seçer (kurum çalışanlarına ulaşması kolay olduğu için çoğunlukla Linkedin'i tercih ederler) ve daha sonra burada bu kişi adına sahte bir profil oluşturarak bu kişinin bağlantıları ile iletişime geçerek bu kişiyi taklit ederek bağlantı kurdukları kişileri kandırarak hassas bilgilere erişmeye ve oradan sistemlere sızmaya çalışırlar. Bu saldırıların önüne geçmek isteyen kurumsal firmalar, çalışanlarının iş ile ilgili sosyal ağlarda (Linkedin) profillerini genele açmamaları ve kurumal e-posta adresleri ile bu tür sitelere üye olmamaları konularında uyarırlar.

Genele açık Twitter hesabım olduğu için birgün Twitter üzerinden kendimle ilgili ne tür bilgiler elde edebileceğini merak ettim ve bu zamana dek göndermiş olduğum mesajları arşivleyen bir site aradım ancak bulamadım. Kafaya koyan biri bugüne kadar göndermiş olduğum tüm mesajları elde edebilir mi diye kafa patlatmaya başladım ve ufak bir program hazırlamaya başladım ve sonunda ortaya hedef twitter hesabından bugüne kadar gönderilen tüm mesajları toplayan ve kayıt eden twitter_crawler.py adında bir program ortaya çıkıverdi.

Programa buradan ulaşabilirsiniz.

Askere gitmeden önce hazırlamış olduğum yaylalar yazı dizisinin üçüncüsü burada son bulurken herkese güvenli günler dilerim.

Ekran görüntüsü:


C:\Windows\system32\cmd.exe
==
Twitter Crawler [http://www.mertsarica.com]
==
[+] Running...
[+] Crawled 1. page
[+] Crawled 2. page
[+] Crawled 3. page
[+] Crawled 4. page
[+] Crawled 5. page
[+] Crawled 6. page
[+] Crawled 7. page
[+] Crawled 8. page
[+] Crawled 9. page
[+] Crawled 10. page
[+] Crawled 11. page
[+] Crawled 12. page
[+] Crawled 13. page
[+] Crawled 14. page
[+] Crawled 15. page
[+] Crawled 16. page
[+] Crawled 17. page
[+] Crawled 18. page
[+] Crawled 19. page
[+] Crawled 20. page
[+] Crawled 21. page
[+] Crawled 22. page
[+] Crawled 23. page
[+] Crawled 24. page
[+] Crawled 25. page
[+] Crawled 26. page
[+] Crawled 27. page
[+] Crawled 28. page
[+] Crawled 29. page
[+] Crawled 30. page
[+] Crawled 31. page
[+] Crawled 32. page
[+] Crawled 33. page
[+] Crawled 34. page
[+] Crawled 35. page
[+] Crawled 36. page
[+] Crawled 37. page
[+] Crawled 38. page
[+] Crawled 39. page
[+] Crawled 40. page
[+] Crawled 41. page
[+] Crawled 42. page
[+] 806 tweets crawled and stored in tweets.txt successfully :)
C:\Users\Mert\Desktop>