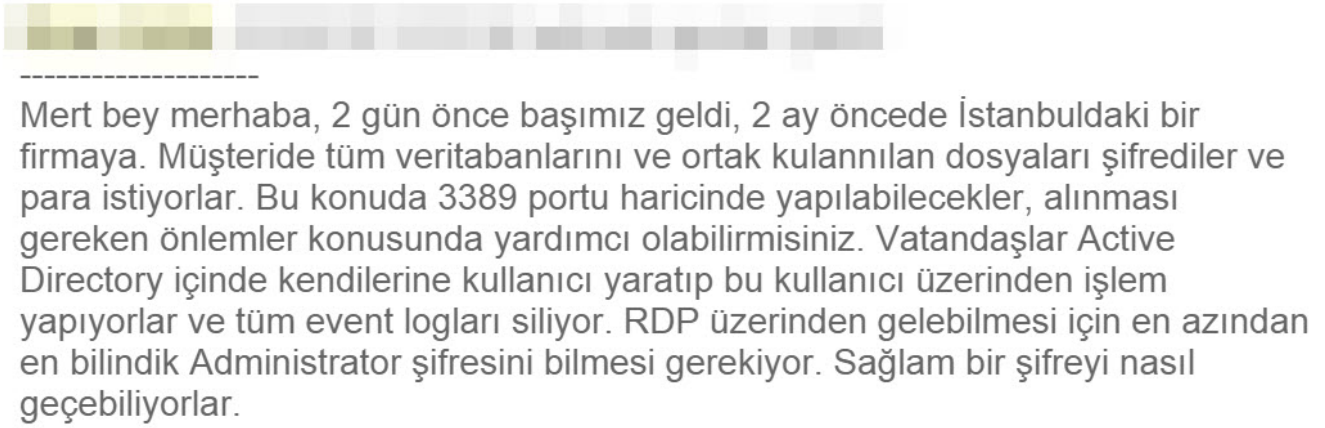
Tuzak Sistem ile Hacker Avı

written by Mert SARICA | 3 July 2017
If you are looking for an English version of this article, please visit here.

Etrafımdaki tanıdığım, tanımadığım çok sayıda kişiden son yıllarda şu soruyu duymaya başladım, “Verilerimi şifrelediler, para istiyorlar, ne yapabilirim ? Kimden yardım alabilirim ?”. Bunu, yıllarca yapılan uyarıları dikkate almayıp, emniyet kemeri takmadan yola çıkıp, hızla duvara toslayıp daha sonra kolunu kaybeden bir kişinin “kolumu kaybettim, ne yapabilirim ?” sorusuna benzetiyorum. Bazı hataların maalesef telafisi ya kolay olmuyor ya da olmuyor. Şifreleme zararlı yazılımlarının cirit attığı siber dünyada, verilerinizi periyodik olarak yedeklemez, sistemlerinizde/cihazlarınızda güçlü parolalar kullanmaz (büyük, küçük harf ve özel karakter kullanma gibi), sistemlerinizin güvenliğini sıkılaştırmazsanız (hardening), muhakkak art niyetli birilerinin doğrudan ya da dolaylı olarak hedefi haline gelmeniz çok uzun sürmez. Geçmişten, günümüze doğru yapmış olduğum güvenlik araştırmalarına bakacak olursanız aslında ne demek istediğimi daha net anlayabilirsiniz.



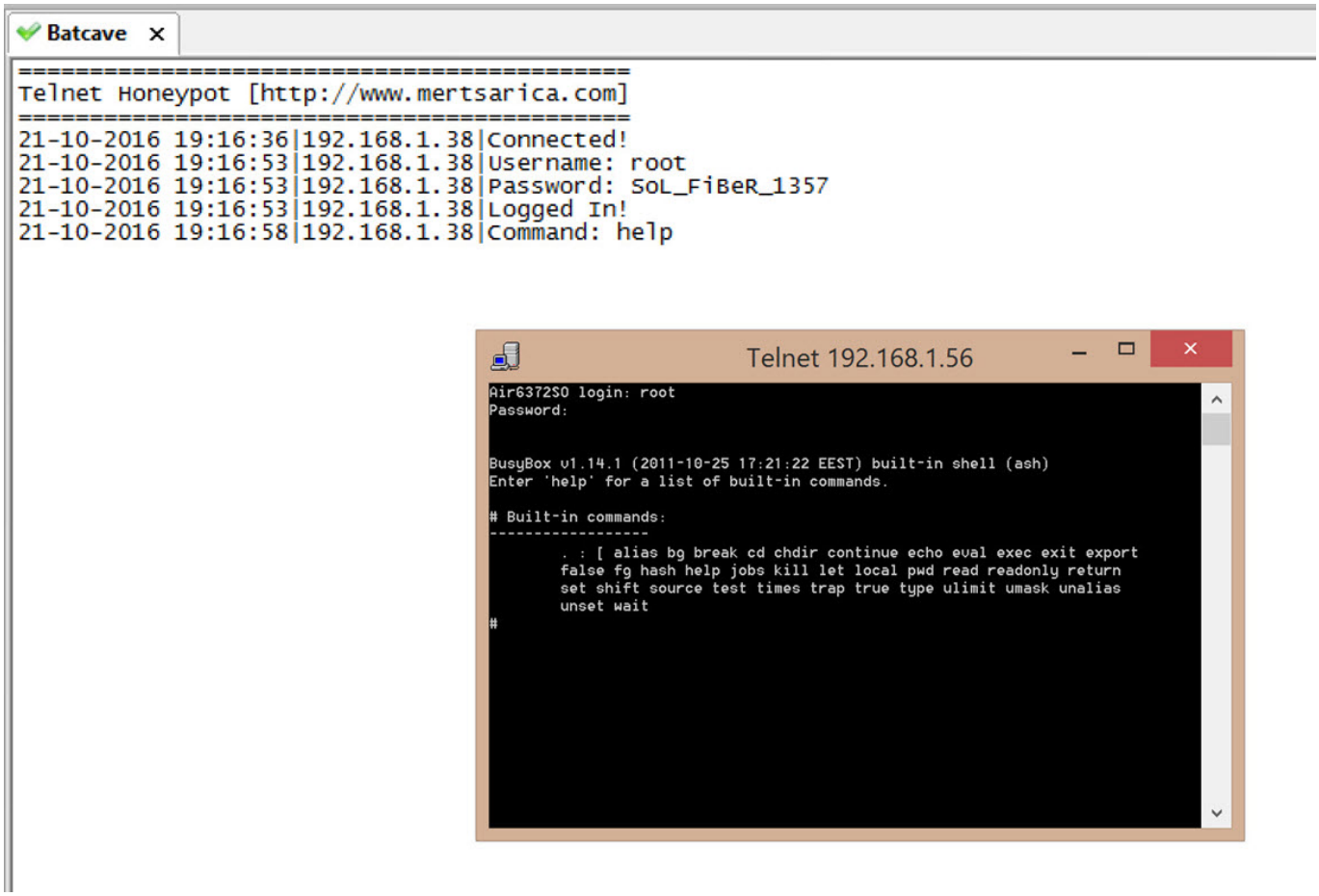
Mert bey merhaba, 2 gün önce başımız geldi, 2 ay öncede İstanbuldaki bir firmaya. Müşteride tüm veritabanlarını ve ortak kulannılan dosyaları şifrediler ve para istiyorlar. Bu konuda 3389 portu haricinde yapılabilecekler, alınması gereken önlemler konusunda yardımcı olabilirmisiniz. Vatandaşlar Active Directory içinde kendilerine kullanıcı yaratıp bu kullanıcı üzerinden işlem yapıyorlar ve tüm event logları siliyor. RDP üzerinden gelebilmesi için en azından en bilindik Administrator şifresini bilmesi gerekiyor. Sağlam bir şifreyi nasıl geçebiliyorlar.

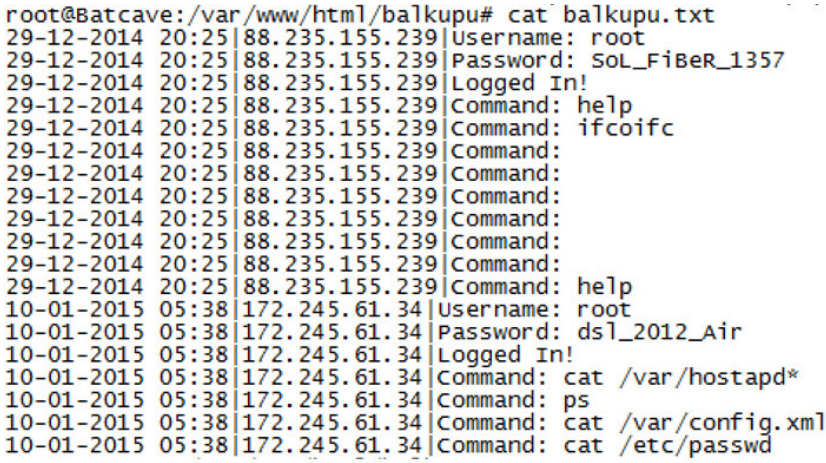
2010 yılında yapmış olduğum ve yazıya döktüğüm Sanal Kuşatma başlıklı blog yazımda, evime kurduğum basit bir honeypot ve aşağıdaki cümle ile dikkat çekmeye çalıştığım nokta, bugün sanal dünyada son kullanıcıların yaşadığı sorunların hemen hemen ayak sesleri gibiydi.

“Honeypot kayıtlarından edindiğim bilgileri kısaca özetleyecek olursam honeypot üzerinde yer alan 11 bağlantı noktasından bir tanesine internete

açıldıktan 12 dakika sonra ilk bağlantı gerçekleşmiş ve 5 saat içinde toplamda honeypota 8 farklı ülkeden, 14 farklı ip adresinden iletişim kurulmuştur.”

2014 yılında ise Air6372SO Varsayılan Hesap Doğrulaması başlıklı bir diğer blog yazımda, donanım yazılımlarına gömülen kullanıcı adı ve parolaların son kullanıcılar olarak güvenliğimizi nasıl tehlikeye atabileceğine dikkat çekmeye çalışmıştım. Yazının akabininde de, internetten gelen bağlantıları kabul edecek şekilde tasarladığım sahte Telnet Honeypot aracını sessiz sedasız hayata geçirdim. Kendisini Airties modemin konsol arabirimiymiş gibi tanıtan ve yazıda bahsi geçen gömülü parolalarla bağlantı kurmaya çalışanları kayıt altına alan bu araç ile yazının yayınlanmasından kısa bir süre sonra hem yurtiçinden hem de yurtdışından bağlantı kurulduğunu gördüm. Bunlardan birinde, İngiltere’den bağlantı kuran bir ip adresi (172.245.61.34), WiFi erişim noktası adını ve parolasını çalıp, sırra kadem bastı. Sebebi üzerine biraz düşününce, art niyetli kişilerin şifre kırmak amacıyla parola sözlüğü oluşturmak veya Wifi modeminiz üzerinden yeri geldiğinde siber suç işlemek için bu bilgileri toplamış olma ihtimalleri yüksek olabilirdi.





2016 yılının sonuna doğru ise yazımın başında belirttiğim şifreleme yöntemi kullanan fidyecilerin izledikleri yöntemleri açıklığa kavuşturmaya karar verdim. Rivayete göre art niyetli kişiler Türkiye'nin ip bloğunu Nmap vb. bağlantı noktası (port) tarama araçları ile tarıyorlar ve ardından internete açık olan Remote Desktop servisine Ncrack vb. araçlarla sözlük saldırısı (dictionary attack) gerçekleştiriyorlardı. Bu araştırma için bütçemi çok zorlamadan (6 taksit :)) gerekli donanımları toplamaya başladım.

Donanımları topladıktan sonra donanım olarak ortaya 2 GHZ hızında işlemcisi, 8 GB RAM'i ve 120 GB SSD diski olan bir tuzak sistem çıktı. Bunun üzerine ilk iş olarak ücretsiz olan ESXi sanallaştırma sistemini kurdum. Onun üzerine de üzerinde sahte muhasebe uygulaması bulunacak olan bir Windows 7 (Honeypot), tuzak sistemi hackleyen art niyetli kişilerin ağ trafiğini izlemek ve internet bağlantısını kısıtlamak amacıyla (malum sanal sistemimi başka suçlara alet etmelerini istemezdim) Ubuntu işletim sistemi (Batcave) kurdum. Windows 7'yi yerel ağda izole edip, internete bağlanabilmesi için Ubuntu'yu da vekil sunucu (ssl inspection proxy) yaptım.

Gigabyte GB-BACE-3150 Intel Celeron N3150 2.08GHz Mini Masaüstü Bilgisayar

%31 indirim ~~678,64 TL~~ **468,91 TL**

★★★★½ Yorum (4) | Yorum Yap

Peşin Fiyatına 9 x 52,10 TL | **Taksit Tablosu**

Satıcı: Hepsiburada

- 1 Adet + Sepete Ekle

En geç **9 Mayıs Pazartesi** günü kargoda

Bugün Teslimat Seçeneği

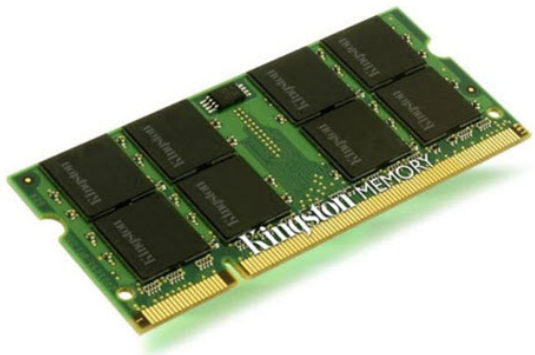
Favori Listeme Ekle | Karşılaştır | Fiyat Alarmı

Diğer Satıcılar - Tümü (2)

Fiyat / Satıcı	Kargo / Kampanya	
447,21 TL Teknolium	• En geç **9 Mayıs Pazartesi** günü kargoda • Bu mağazada kargo bedava!	Sepete Ekle

Ürün Açıklaması | Yorumlar (4) | Taksit | İade Koşulları | Tüm Satıcılar (2)

Marka	Gigabyte
İşlemci Tipi	Intel Celeron
İşlemci Hızı	2 GHz
İşlemci Cache	2 MB cache
Ram Tipi	DDR3
Ekran Kartı Tipi	Dahili Ekran Kartı
Ekran Kartı Modeli	Paylaşımlı
Monitör	Yok
3D Desteği	Yok
Wireless Özelliği	802.11 n
Kimin Seçimi	Günlük



Kingston ValueRam 8GB 1600MHz DDR3 Notebook Ram (KVR16LS11/8)

%27 indirim ~~168,10 TL~~ **123,06 TL**

★★★★★ Yorum (21) | Yorum Yap

Peşin Fiyatına 6 x 20,51 TL | **Taksit Tablosu**

Satıcı: Hepsiburada

- 1 Adet + Sepete Ekle

En geç **9 Mayıs Pazartesi** günü kargoda

Bugün Teslimat Seçeneği

Favori Listeme Ekle | Karşılaştır | Fiyat Alarmı

Diğer Satıcılar - Tümü (7)

Fiyat / Satıcı	Kargo / Kampanya	
115,50 TL Nethouse	• En geç **9 Mayıs Pazartesi** günü kargoda	Sepete Ekle
115,64 TL Pazarbizde	• En geç **11 Mayıs Çarşamba** günü kargoda	Sepete Ekle

Ana Sayfa > Bilgisayarlar > Veri Depolama Ürünleri > SSD Solid State Drive > Sandisk SSD Solid State Drive

Sandisk SSD Plus 120GB 520MB-180MB/s Sata3 2.5" SSD (SDSSDA-120G-G25)

%40 indirim ~~199,00 TL~~ **119,00 TL**

★★★★½ Yorum (70) | Yorum Yap

Peşin Fiyatına 6 x 19,83 TL | **Taksit Tablosu**

Satıcı: Hepsiburada

- 1 Adet + Sepete Ekle

En geç **9 Mayıs Pazartesi** günü kargoda

Bugün Teslimat Seçeneği

Favori Listeme Ekle | Karşılaştır | Fiyat Alarmı

Diğer Satıcılar - Tümü (9)

Fiyat / Satıcı	Kargo / Kampanya	
122,90 TL Webdenal	• En geç **9 Mayıs Pazartesi** günü kargoda • Bu mağazada kargo bedava!	Sepete Ekle
123,90 TL Cesur Bilişim	• En geç **10 Mayıs Salı** günü kargoda • Bu mağazada kargo bedava!	Sepete Ekle

192.168.1.54 - vSphere Client

File Edit View Inventory Administration Plug-ins Help

Home > Inventory > Inventory

192.168.1.54
Batcave
Honeypot

localhost.localdomain VMware ESXi, 6.0.0, 3620759

Getting Started | Summary | Virtual Machines | Resource Allocation | Performance | Configuration | Users | Events | Permissions

Name, State or Guest OS contains: Clear

Name	State	Provisioned Space	Used Space	Host CPU - MHz	Host Mem - MB	Guest Mem - %	Notes
Batcave	Powered On	45,23 GB	25,24 GB	178	1124	6	
Honeypot	Powered On	125,26 GB	65,27 GB	893	2096	33	

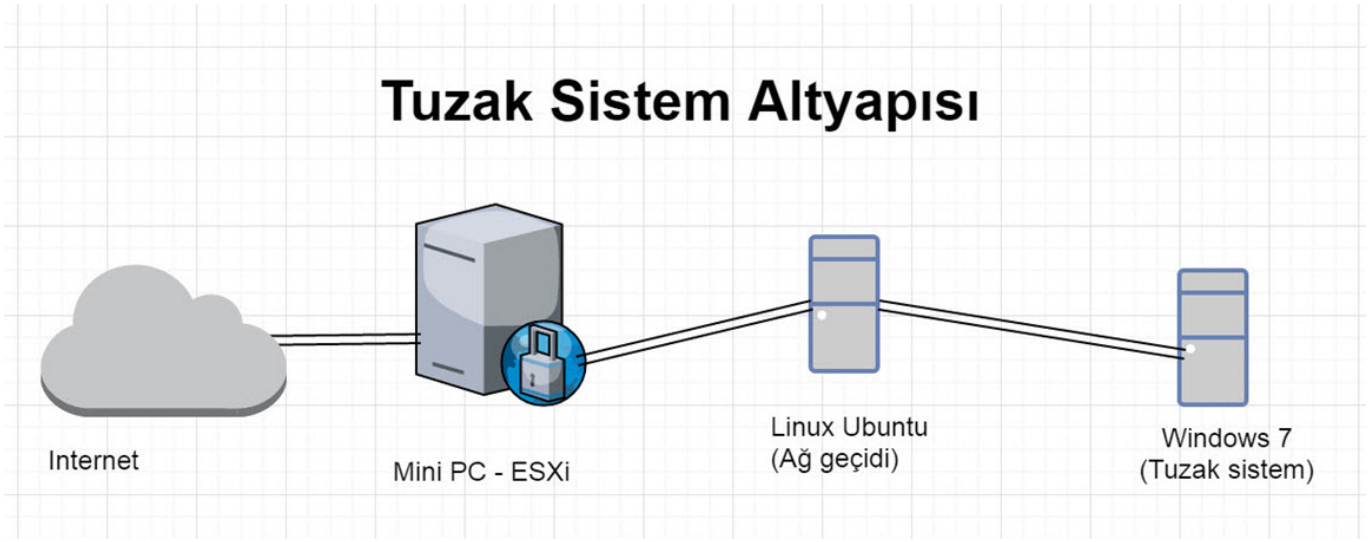
Recent Tasks

Name, Target or Status contains: Clear

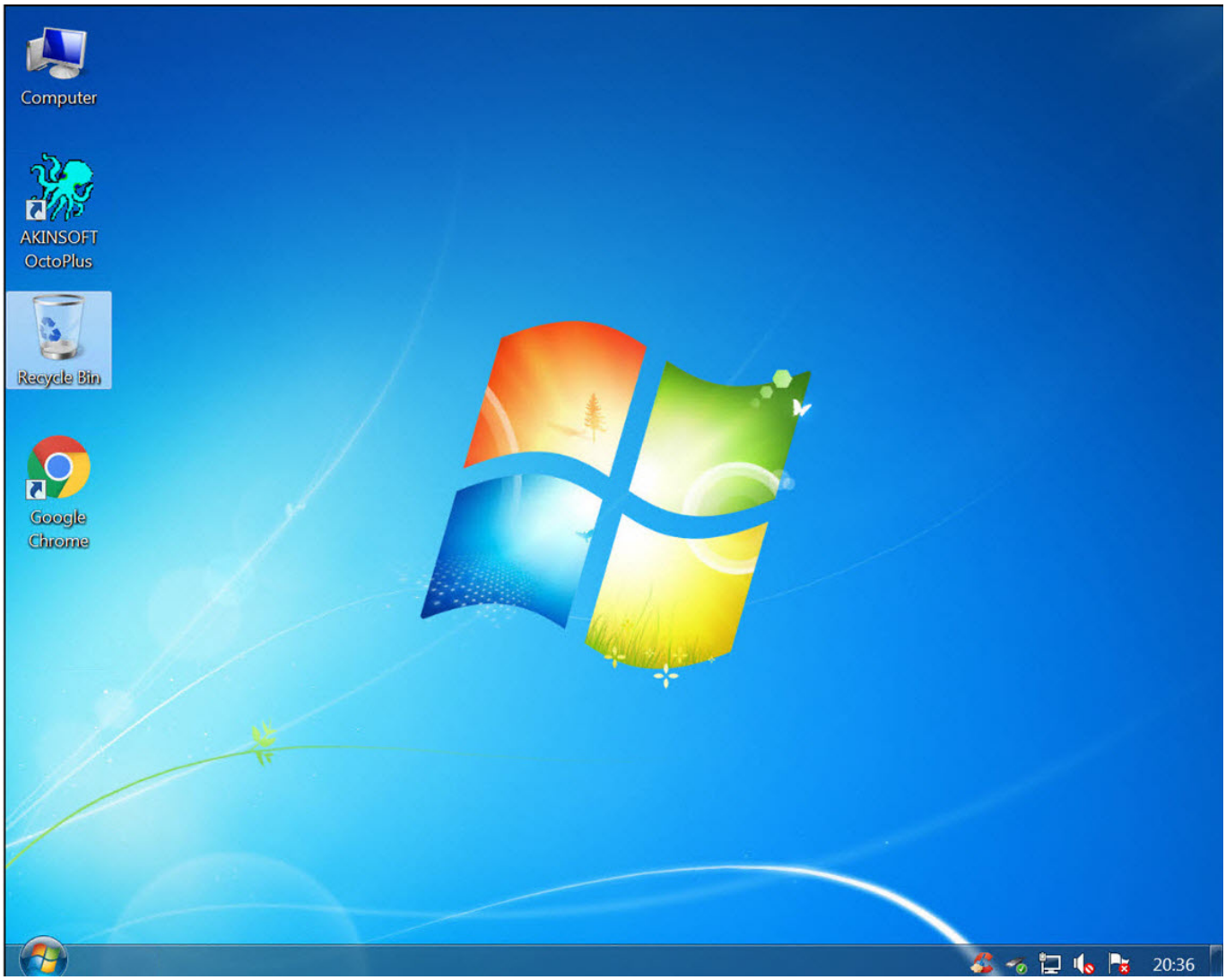
Name	Target	Status	Details	Initiated by	Requested Start Ti...	Start Time	Completed Time

Tasks

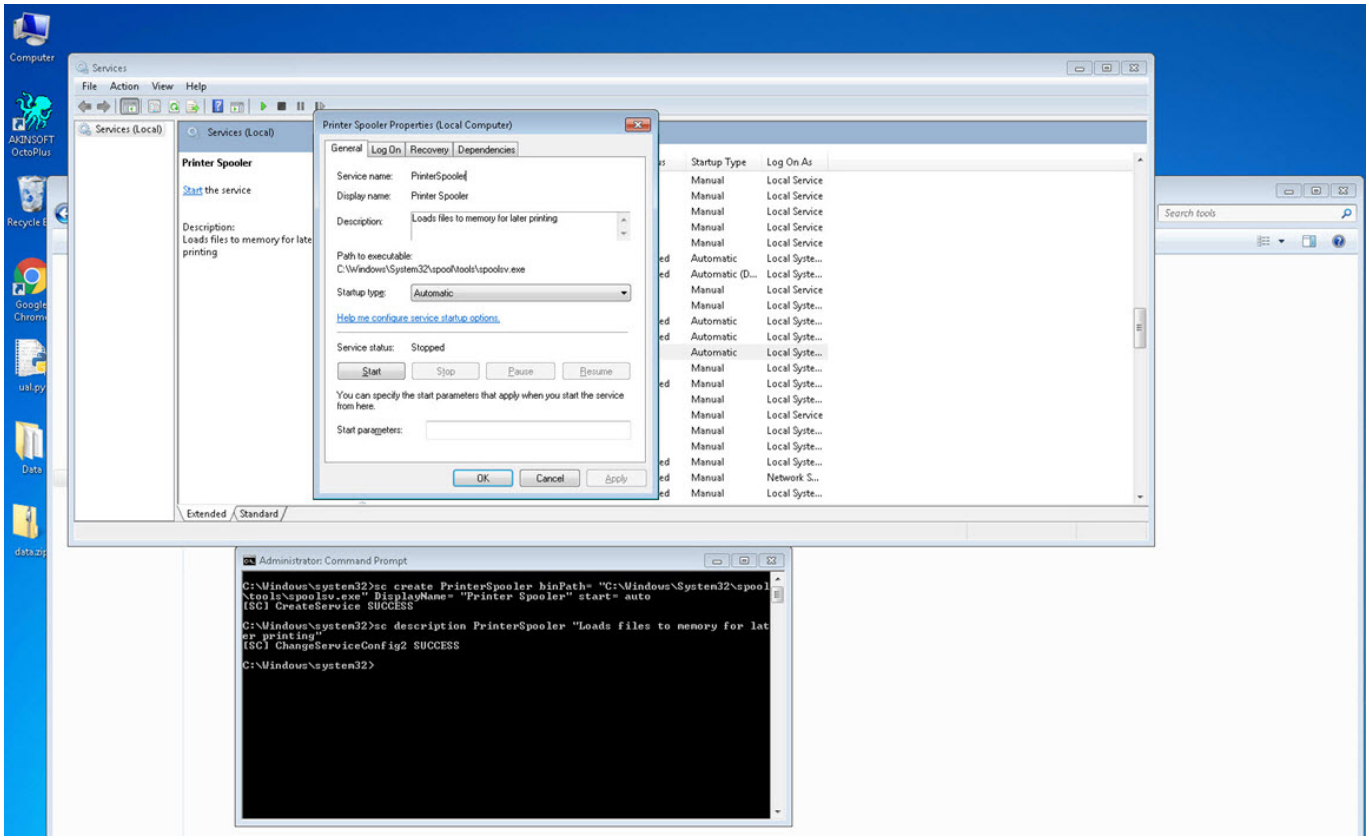
To release cursor, press CTRL+ALT root



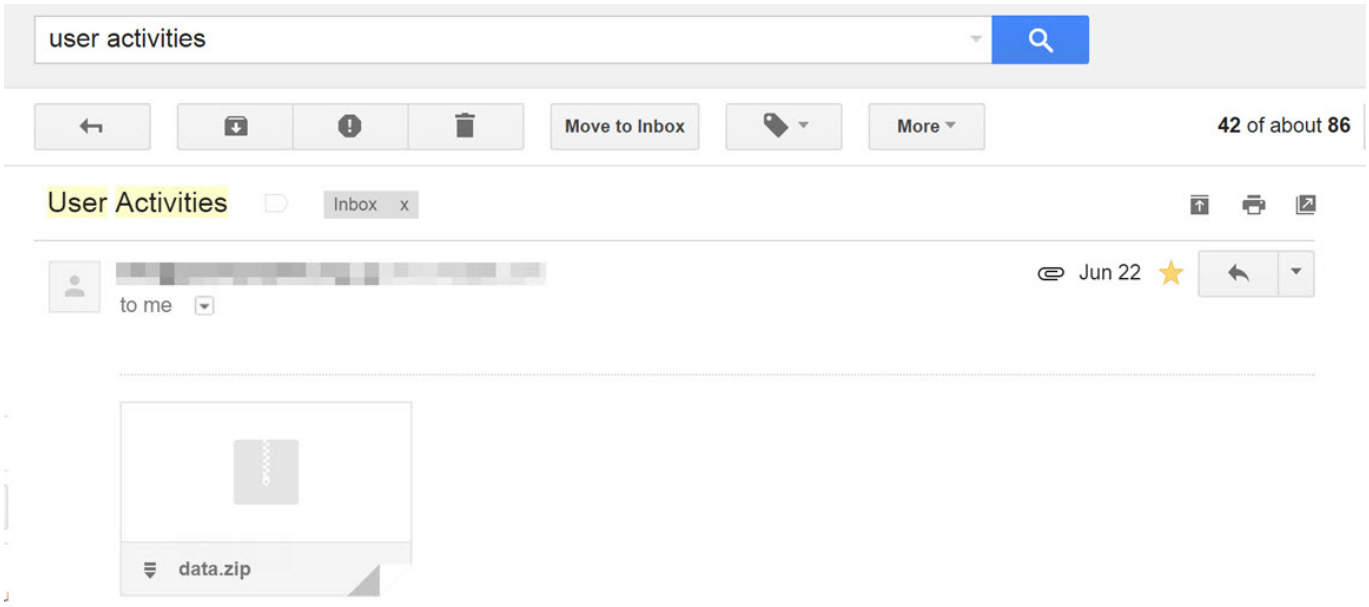
Tuzak sistemi art niyetli kişiler için çekici hale getirmek amacıyla Windows 7 yüklü sisteme yüklemek üzere bir muhasebe yazılımı arayışına başladım. Hangi muhasebe yazılımının olacağına karar vermek için ise verileri şifrelenen mağdurlardan edindiğim bilgilerden faydalanarak tercihimi Akınsoft firmasının OctoPlus yazılımından yana yaptım.



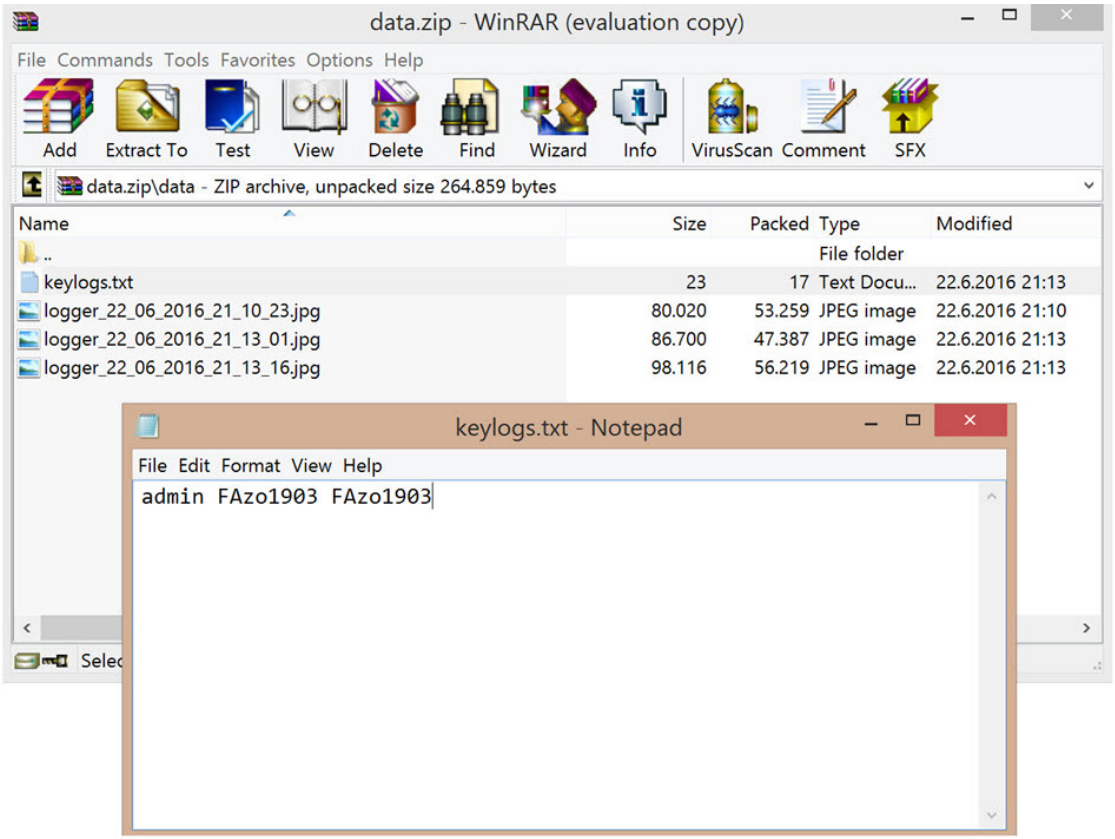
Sıra tuzak sistemi tuzak yapacak olan aracı tasarlamaya geldiğinde her zaman olduğu gibi Python ile Windows üzerindeki kullanıcının tüm hareketlerini kayıt altına alan (tuş kaydı, video kaydı, ekran görüntüsü alma, pano (clipboard) kopyalama) ve video dosyası hariç geri kalan tüm bilgileri her 5 dakikada bir e-posta ile gönderen UAL (User Activity Logger) (kötüye kullanılmaması adına kaynak kodunu yayınlamama kararı aldım, üzgünüm.) adını verdiğim bir araç hazırladım. Tuzak sisteme bağlanan art niyetli kişileri uyandırmama adına işletim sistemi üzerinde Python27 klasörü başkta olmak üzere çeşitli klasörleri gizledim. Ardından derlediğim UAL.py aracının adını spoolsv.exe olarak değiştirip, her oturumda yeniden çalıştırılacak şekilde Windows servisi olarak kayıt ettim.



Tuzak sistemin yönetici parolasını muhasebe yapıp, modem üzerinden internet erişimine açtıktan sonra 6 ay boyunca bu sistemi izlemeye başladım. 6 ay süresince tuzak sisteme düşenler sayesinde sistemi iyileştirme adına epey bir yol katettim. Örneğin çoğu art niyetli kişi muhasebe dosyalarını şifrelemeden önce dosyaların değiştirilme tarihine bakıp, muhasebe programının aktif olarak kullanılıp kullanılmadığını kontrol ediyordu. Her ne kadar sözlük saldırısı ile tuzak sistemin yönetici parolasını kısa bir süre zarfında bulanlar olsa da, eşi dosta hedef alıp medyaya konu olan, verileri şifreleyip, not bırakan fidyecilerden birinin tuzak sistemime düşmesi yaklaşık 6 ay sürdü.


user activities
Move to Inbox
More
42 of about 86
User Activities
Inbox x
to me
Jun 22
data.zip

data 6 items
keylogs.txt
logger_22_06_2016_21_19_35.jpg
logger_22_06_2016_21_19_51.jpg
logger_22_06_2016_21_20_06.jpg
logger_22_06_2016_21_20_37.jpg
logger_22_06_2016_21_20_53.jpg


data.zip - WinRAR (evaluation copy)
File Commands Tools Favorites Options Help
Add
Extract To
Test
View
Delete
Find
Wizard
Info
VirusScan
Comment
SFX
data.zip\data - ZIP archive, unpacked size 264.859 bytes
Name
Size
Packed
Type
Modified
..
File folder
keylogs.txt
23
17
Text Docu...
22.6.2016 21:13
logger_22_06_2016_21_10_23.jpg
80.020
53.259
JPEG image
22.6.2016 21:10
logger_22_06_2016_21_13_01.jpg
86.700
47.387
JPEG image
22.6.2016 21:13
logger_22_06_2016_21_13_16.jpg
98.116
56.219
JPEG image
22.6.2016 21:13
keylogs.txt - Notepad
File Edit Format View Help
admin FAzo1903 FAzo1903

Bilgisayar korsanlarına operasyon

DHA 03 Temmuz 2013 - 12:13 | Son Güncelleme : 03 Temmuz 2013 - 12:14

İstanbul Siber Suçlarla Mücadele Şube Müdürlüğü 3 yıl önce internet üzerinden şirketlerin ana bilgisayar sunucusuna girerek sistemdeki tüm belgelerini ele geçiren bir şebekeyle ilgili çalışma başlattı.

PAYLAŞ A Yorum yaz

Ele geçirilen bilgileri şirketin ana bilgisayarındaki tek dosyaya koyan şebeke bu dosyayı şifreleyerek şirket çalışanlarının içinde, ihracat, ithalat, muhasebe ve insan kaynaklarının da bulunduğu bilgilere ulaşmalarına engel oldular. Şifre karşılığında şirketten para isteyen aksi halde şirket bilgilerini internette deşifre edeceğini belirten şebeke elemanları, yetkililerin kendilerine ulaşması için bilgisayarda oluşturulan dosyada "crypteks@hotmail.com , money4ptr.pan @gmail.com" gibi benzer isimlerde 19 mail adresi bıraktı. Şebeke, para ödeyen firmalara şifresini verirken ödemeyenlerin bilgilerini bir internet sitesinde yayınladı.

273 ŞİRKETİN BİLGİSAYARINI ELE GEÇİRDİLER YAPTIKLARI 2 HATA YAKALATTI

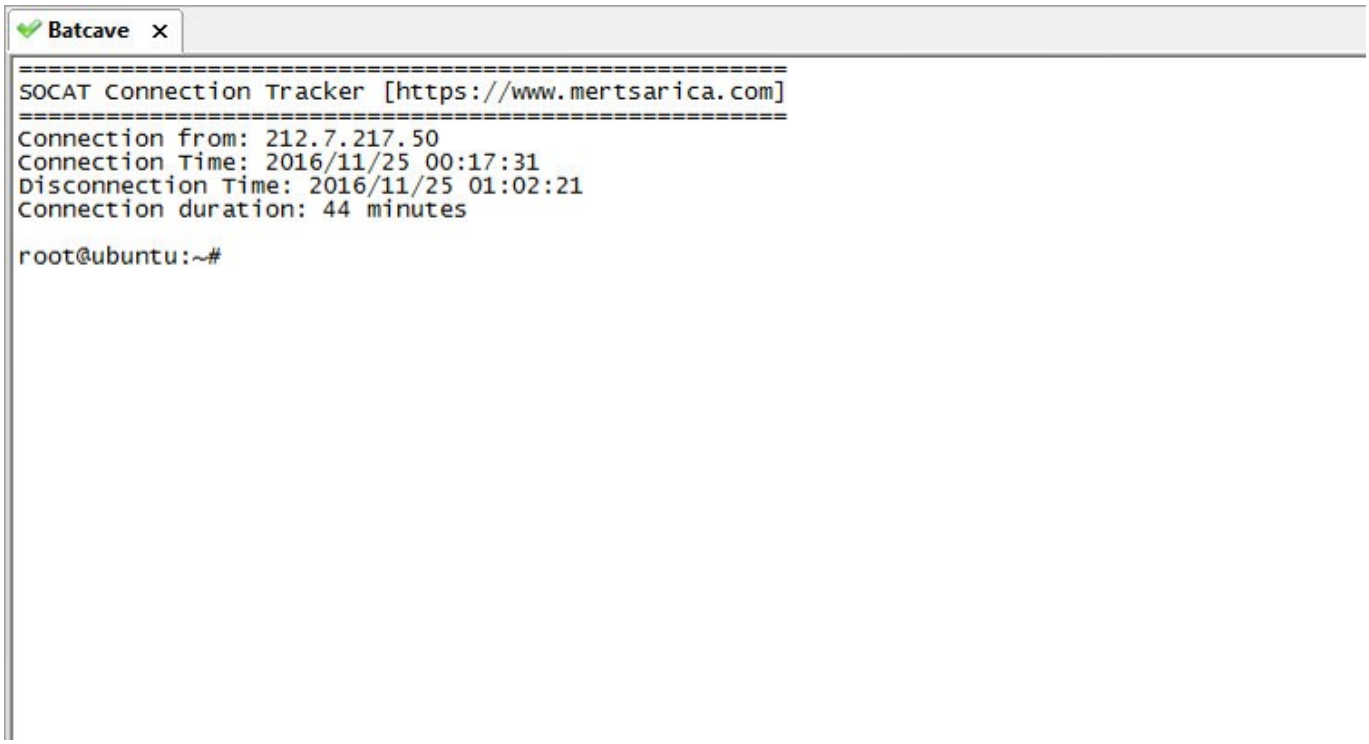
Polis 2011 yılından beri yaptığı araştırmada, incelenen 273 olayın 271'inde bir ize ulaşılamadığı ancak 2 olayda yapılan hata sayesinde şebeke ele başı S.B.'ye ulaşıldı. Ukrayna'da yaşayan Türk vatandaşı bilgisayar mühendisi S.B.'nin 3 ay önce Türkiye'ye giriş yaptığı belirlendi. Polis S.B.'nin irtibatlarını belirlemek için şebeke elebaşını adım adım takip etti. Antalya'da bir otelde tatil yapan S.B.'nin yurt dışına çıkma hazırlığında olduğu belirlenince 3 aylık takibin ardından geçtiğimiz hafta operasyon startı verildi. 10 ilde gerçekleştirilen operasyonlarda 20 kişi gözaltına alındı. Gözaltına alınan 15 kişi polis sorgusunun ardından serbest kalırken, 4 kişi savcılık tarafından serbest bırakıldı. Şantaj ve bilişim sistemlerine hukuka aykırı olarak girmek gibi suçlardan hattında işlem yapan S.B. ise tutuklanarak cezaevine gönderildi. Polis olayla ilgili yurt dışında yaşayan bazı bilgisayar korsanlarının yakalanması için çalışmalarına devam ediyor.

55 ŞİRKETTEN 87 BİN 684 DOLAR ALDILAR

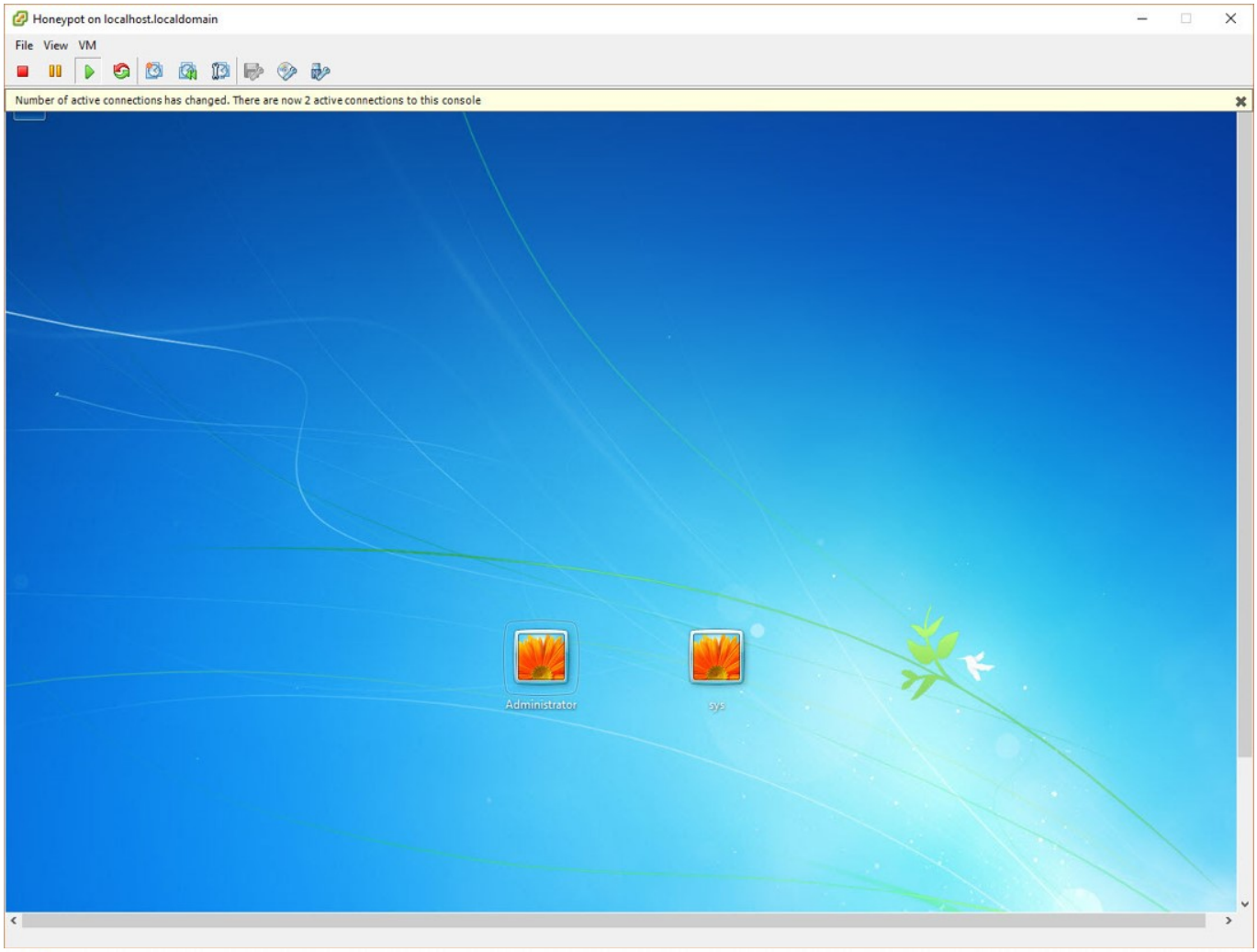
Polis şebekenin para aldığı şirketlerle ilgili çalışmalarına devam ederken, şebekenin, şu ana kadar yapılan tespitlerde 55 şirketten 87 bin 684 Dolar alındığı belirlendi. Paraların şebekenin talebi üzerine Rusya, Ukrayna, Çin Vietnam, Peru gibi ülkelerdeki hesaplara havale edildiği belirlendi. Bu ülkelere havale edilen paralarında farklı şebekeler aracılığı ile çekilerek komisyon karşılığı S.B.'nin adamlarına aktarıldığı iddia edildi.

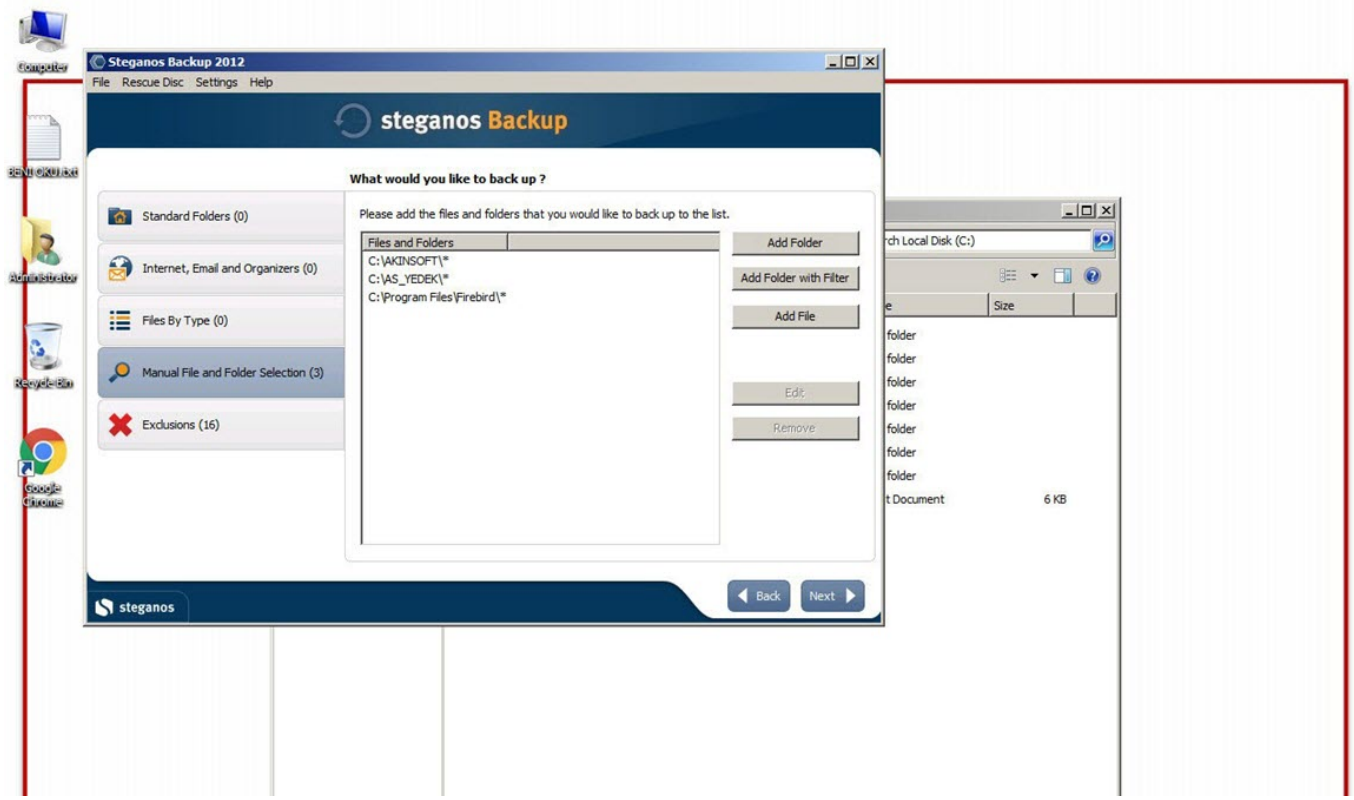
Tuzak sisteme bağlananların IP adreslerini ve sisteme ne kadar süre ile bağlı kaldıklarını öğrenebilme adına Remote Desktop servisine internetten erişim vermek yerine, Ubuntu (Batcave) üzerinden yönlendirme yapmaya karar verdim. Bunun için Ubuntu'nun 3389. bağlantı noktasına (port) gelen tüm istekleri, socat aracı ile tuzak sistemin 3389. bağlantı noktasına yönlendirdim. Socat aracının detaylı kayıt özelliğini yorumlaması pek pratik olmadığı için de

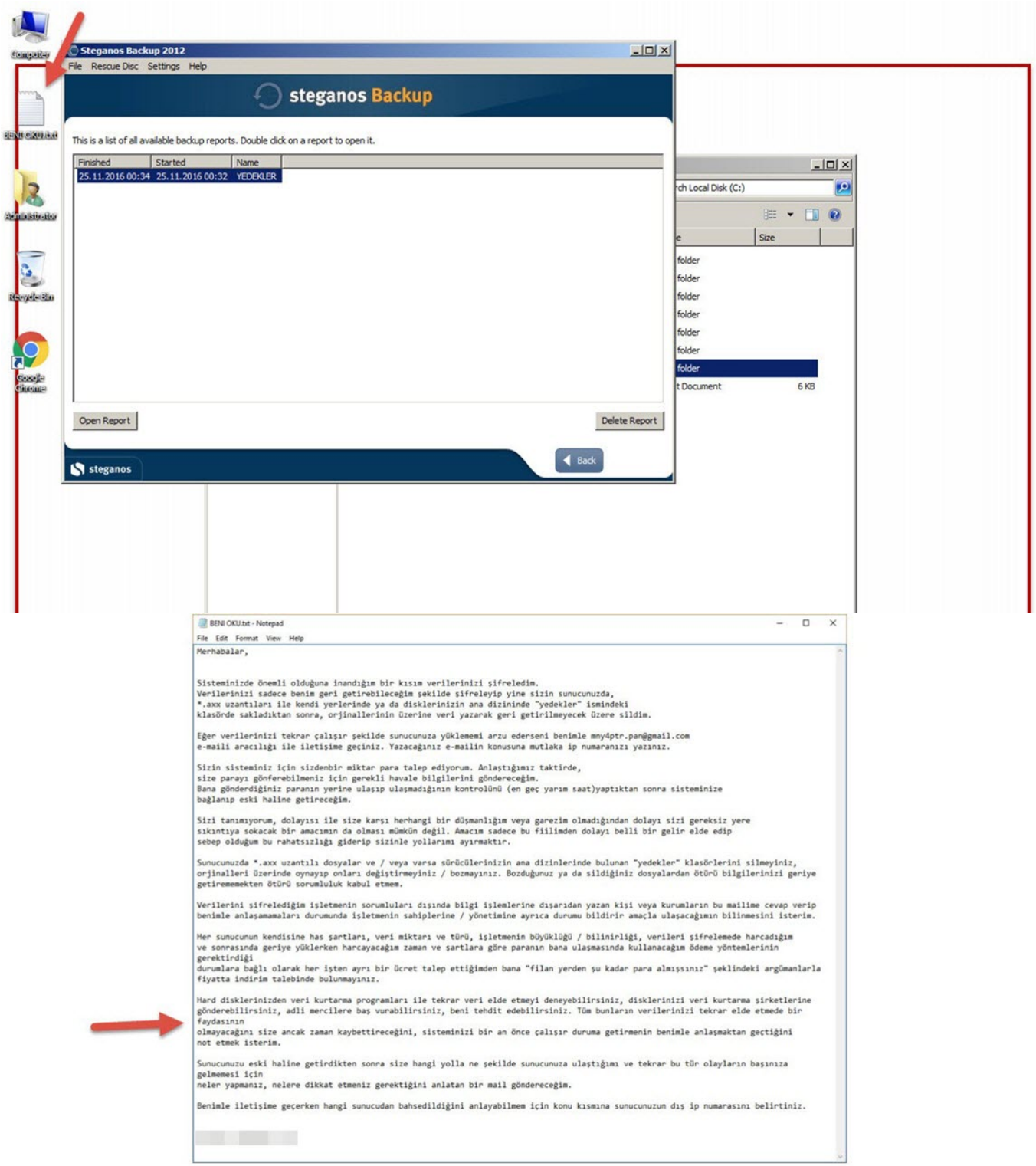
Python ile Socat Connection Tracker adında yardımcı bir araç hazırladım.



Bir sabah uyandığımda e-posta kutumda tuzak sistem tarafından gönderilmiş çok sayıda e-posta olduğunu farkettim. Bu durum ben gece mışıl mışıl uyurken birinin tuzak sistemimi hacklediği anlamına geliyordu. Tuzak sistemin konsoluna ESXi arabiriminden bağlandığımda ilk dikkatimi çeken sistemde Sys isimli farklı bir kullanıcının oluşturulduğuydu. Sisteme giriş yaptığım zaman ise karşıma çıkan Steganos Backup 2012 yedekleme yazılımı ile muhasebe programının klasörlerinin şifreli olarak yedeklendiği ve masaüstünde yer alan not ile uzun zamandan beri beklediğim günün nihayet geldiğini anladım. Bağlantı kuran kişi yukarıda yer alan ekran görüntüsünden de anlaşılacağı üzere tuzak sistemime 44 dakika bağlı kalmıştı.

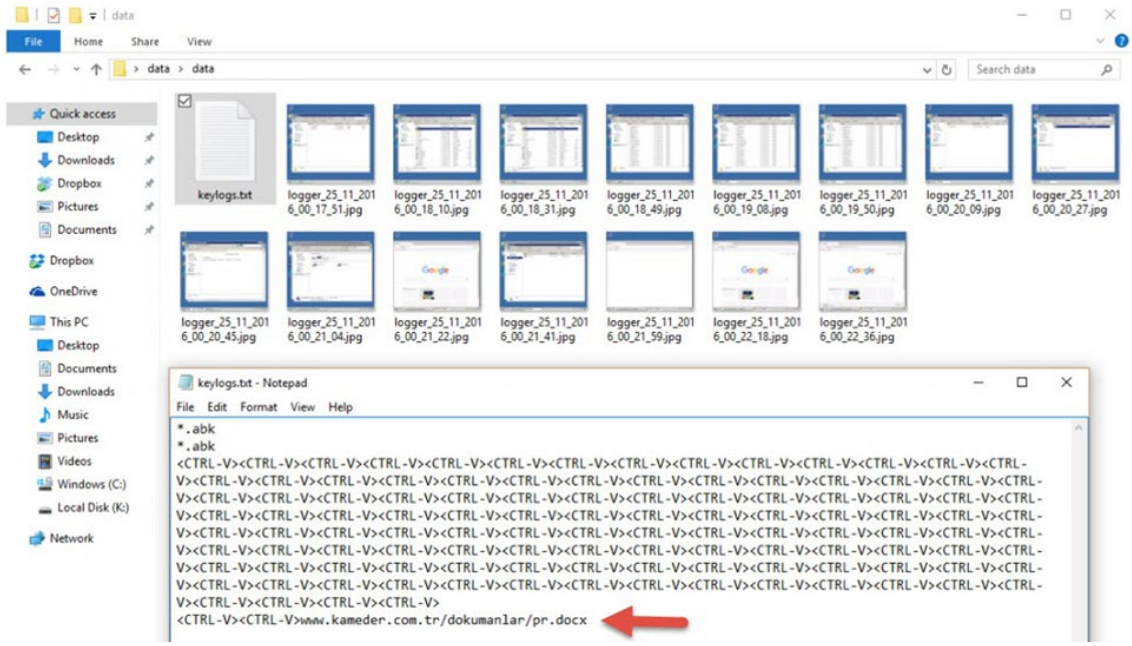

Honeypot on localhost.localdomain
File View VM
Number of active connections has changed. There are now 2 active connections to this console
Administrator
sys

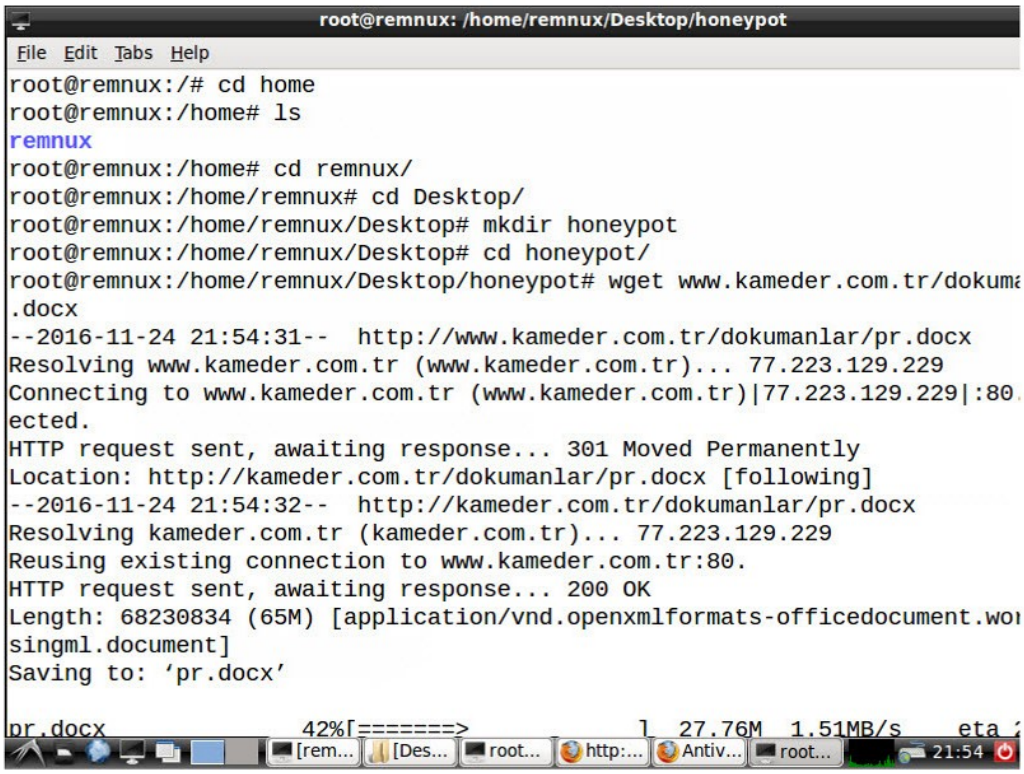

Steganos Backup 2012
File Rescue Disc Settings Help
steganos Backup
What would you like to back up ?
Standard Folders (0)
Internet, Email and Organizers (0)
Files By Type (0)
Manual File and Folder Selection (3)
Exclusions (16)
Please add the files and folders that you would like to back up to the list.
Files and Folders
C:\AKINSOFT*
C:\AS_YEDEK*
C:\Program Files\Firebird*
Add Folder
Add Folder with Filter
Add File
Edit
Remove
steganos
Back
Next
Size
folder
6 KB

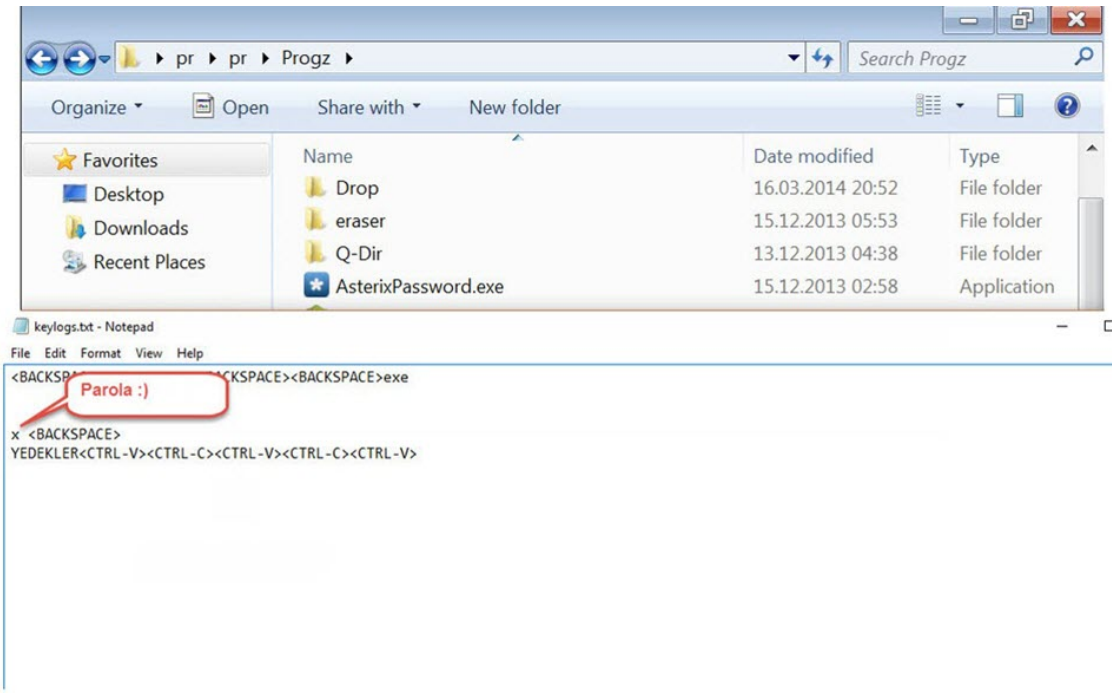


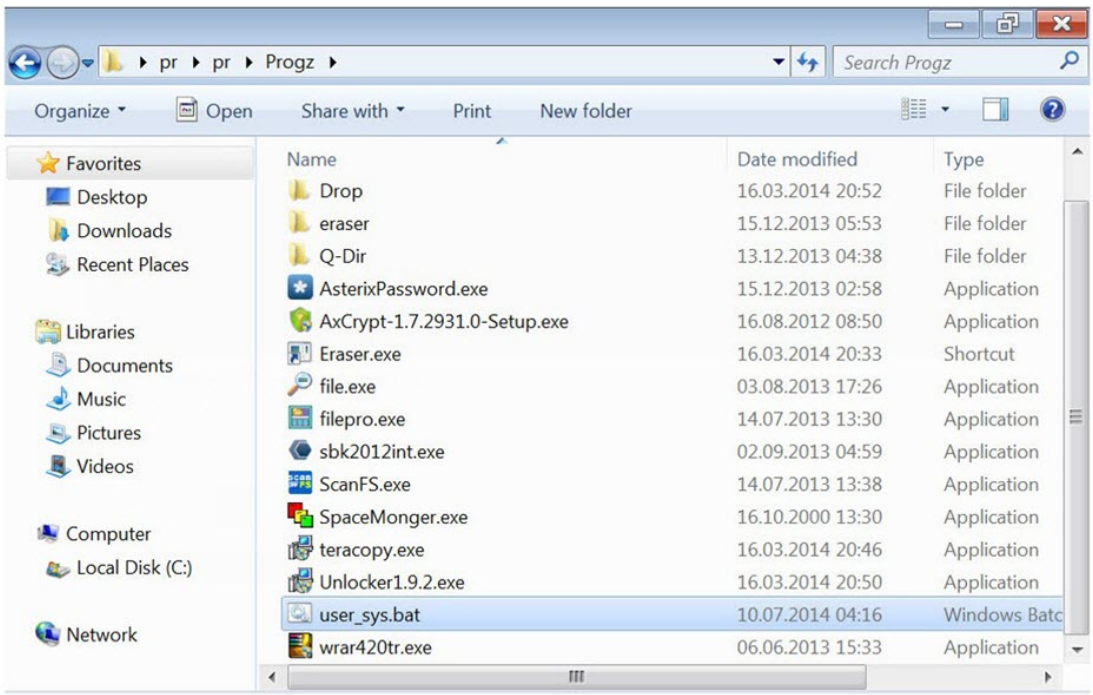
Art niyetli kişiye ait kayıtları incelediğimde kameder.com.tr adresinden (muhtemelen hacklenmiş bir site), pr.docx isimli bir dosya indirdiğini gördüm. 65 MB büyüklüğünde bir belge olması oldukça şüpheli olduğu için bunun bir ZIP dosyasını öğrenmem çok zor olmadı. Bu ZIP dosyasını açmaya çalıştığımda ise bir parola soruluyordu. Parolayı bulmak için ise yine kayıtlara hızlıca göz attığımda, parolanın x olduğunu gördüm. ZIP dosyasını açtığımda art niyetli kişinin hacklediği sistem üzerine yükleyip, çalıştırmak

amacıyla kullandığı tüm araçları karşımda buldum. Sys kullanıcısının parolasını da bir bat dosyası içinde bulduktan sonra şifrelenen dosyalarımın parolasının da olabileceği ihtimaline karşı benzer dosyaları incelemeye devam ettim ancak parola içeren herhangi bir dosya bulamadım.






pr ▸ pr ▸ Progz ▸
Search Progz
Organize
Open
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Name
Date modified
Type
Drop
16.03.2014 20:52
File folder
eraser
15.12.2013 05:53
File folder
Q-Dir
13.12.2013 04:38
File folder
AsterixPassword.exe
15.12.2013 02:58
Application
keylogs.txt - Notepad
File Edit Format View Help
Parola :)
x <BACKSPACE>
YEDEKLER<CTRL-V><CTRL-C><CTRL-V><CTRL-C><CTRL-V>

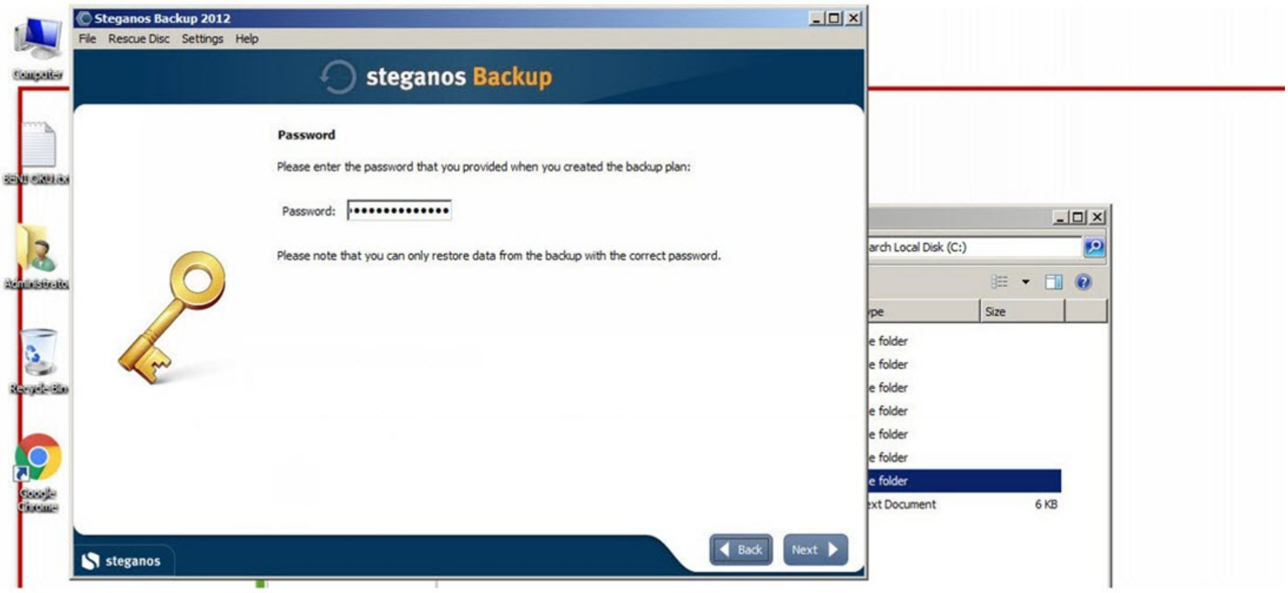

pr ▸ pr ▸ Progz ▸
Search Progz
Organize
Open
Share with
Print
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
Network
Name
Date modified
Type
Drop
16.03.2014 20:52
File folder
eraser
15.12.2013 05:53
File folder
Q-Dir
13.12.2013 04:38
File folder
AsterixPassword.exe
15.12.2013 02:58
Application
AxCrypt-1.7.2931.0-Setup.exe
16.08.2012 08:50
Application
Eraser.exe
16.03.2014 20:33
Shortcut
file.exe
03.08.2013 17:26
Application
filepro.exe
14.07.2013 13:30
Application
sbk2012int.exe
02.09.2013 04:59
Application
ScanFS.exe
14.07.2013 13:38
Application
SpaceMonger.exe
16.10.2000 13:30
Application
teracopy.exe
16.03.2014 20:46
Application
Unlocker1.9.2.exe
16.03.2014 20:50
Application
user_sys.bat
10.07.2014 04:16
Windows Batc
wrar420tr.exe
06.06.2013 15:33
Application

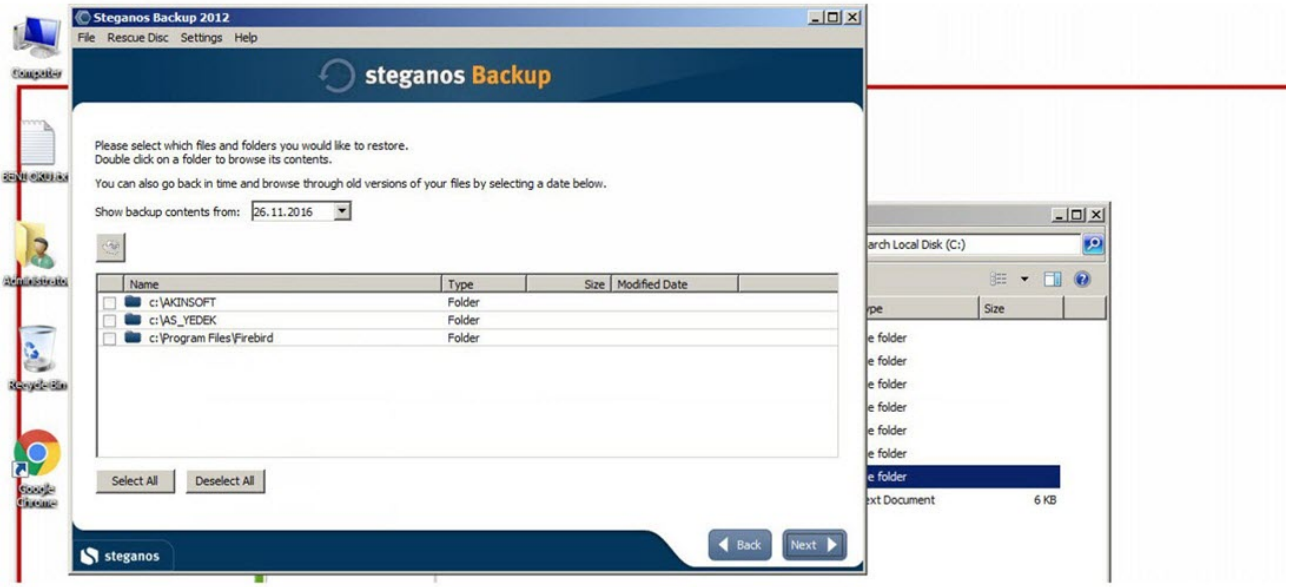
user_sys.bat

```
net user sys Abc+123 /add
net localgroup Administrators sys /add
net localgroup "Remote Desktop Users" sys /add
net accounts /maxpwage:unlimited
pause
```

Tuzak sistem üzerinde kopyala yapıştır ve dosya paylaşımını engellediğim için art niyetli kişinin muhasebe programına ait klasörleri şifrelemek için seçtiği parolayı yazmakta epey zorlandığını gördüm. :) SEMSIPASA ile başlayan uzun parolayı yazmakta epey zorlandıktan sonra karsiyaka ile baslayan bir parola denemiş ve onu da yazamayinca son olarak dvdassanat669- parolasında karar kılmıştı. İzlendiğinden habersiz olan art niyetli kişi, verileri şifreleyip e-posta atılmasını hayal ederken, tuzak sistem sayesinde dvdassanat669- parolası ile şifreyi çözüp, bu konuyu da kendi adıma açıklığa kavuşturmuş oldum.

keylogs.txt - Notepad
File Edit Format View Help
v<CTRL-
V>SEMSIPASAPASASINDASESIBUZUSESICELER<BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE
CKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE>SEMSIPASAPASASINDA
<BACKSPACE><BACKSPACE>SES<BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE>
CKSPACE><BACKSPACE><BACKSPACE><BACKSPACE>SEMSIP<BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE>
PACE><BACKSPACE><BACKSPACE>SEMSIPASAPASASINDASESIBUZUSESICELER<TAB>SEMSIPASAPASASINDASESIBUZUSESICELERkarsiyaka2322040<TAB>karsiyaka323
dvdas<BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE>
BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE>dvdassanat669-<TAB>dvdassanat669-
Elde var 3 parola :)


Steganos Backup 2012
File Rescue Disc Settings Help
steganos Backup
Password
Please enter the password that you provided when you created the backup plan:
Password:
Please note that you can only restore data from the backup with the correct password.
steganos
Back
Next
Size
6 KB



Sonuç itibariyle bu yazıya konu olan fidyecilerle mücadele edebilme adına, periyodik olarak sistemlerinizin yedeğini almak, yedeklerinizi güvenli ortamlarda saklamak, internete açık olan bağlantı noktalarınızı kontrol edip ihtiyaç duymadıklarınızı devre dışı bırakmak ve sistemlerinizde güçlü parolalar kullanmak kısa vadede fidyecilerin kötü emellerine ulaşmalarını zorlaştıracaktır.

Unutmadan, tuzak sistem tarafından art niyetli kişinin verileri şifrelemesi esnasında kayıt ettiği videoyu da aşağıda izleyebilirsiniz.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.