

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.



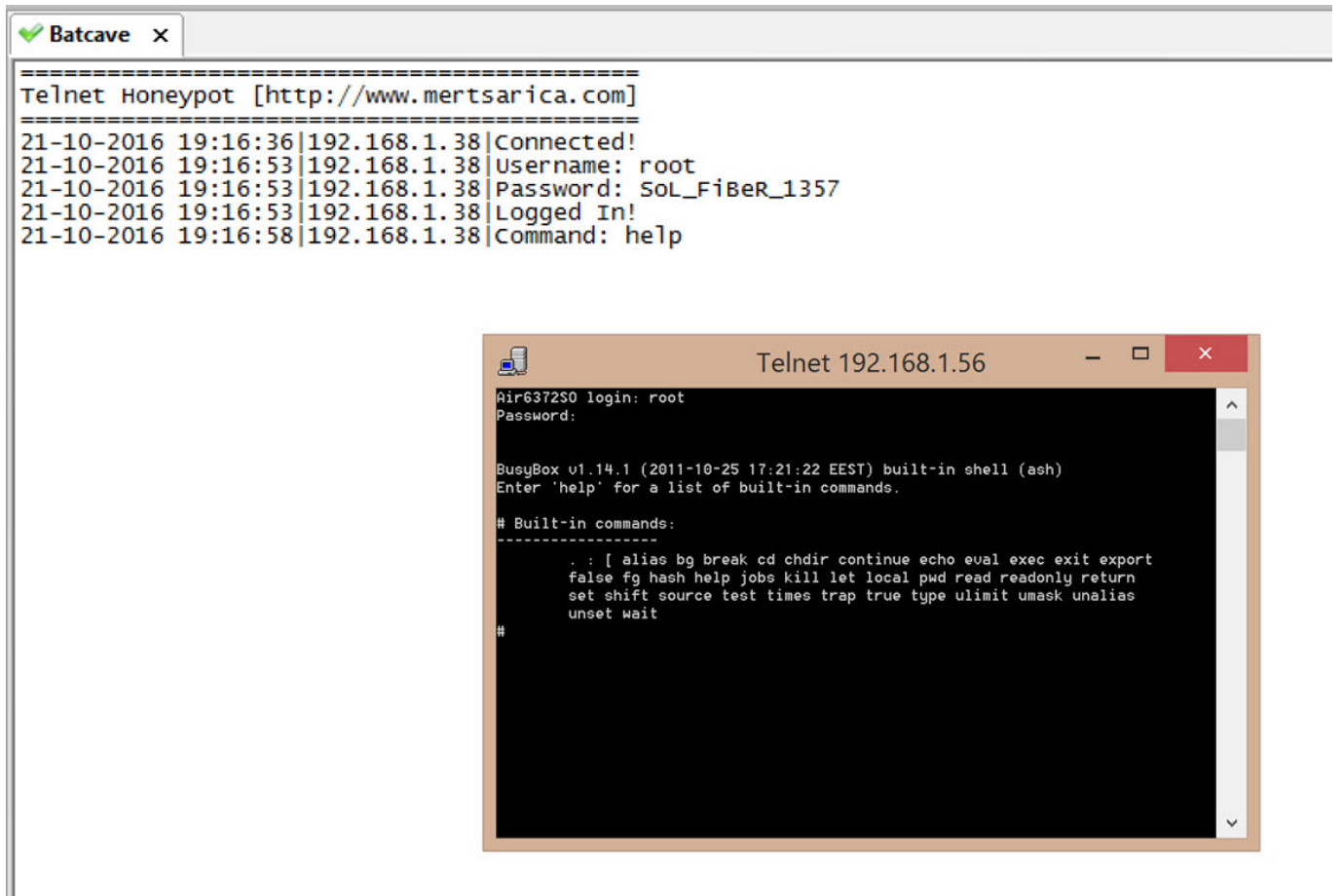
Mert bey merhaba, 2 gün önce başımız geldi, 2 ay öncede İstanbuldaki bir firmaya. Müşteride tüm veritabanlarını ve ortak kullanılan dosyaları şifrediler ve para istiyorlar. Bu konuda 3389 portu haricinde yapılabilecekler, alınması gereken önlemler konusunda yardımcı olabilmisiniz. Vatandaşlar Active 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 Air6372S0 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 akabinde 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.



```
=====
Telnet Honeypot [http://www.mertsarica.com]
=====
21-10-2016 19:16:36|192.168.1.38|Connected!
21-10-2016 19:16:53|192.168.1.38|Username: root
21-10-2016 19:16:53|192.168.1.38|Password: SoL_FiBeR_1357
21-10-2016 19:16:53|192.168.1.38|Logged In!
21-10-2016 19:16:58|192.168.1.38|Command: help
```

```
Telnet 192.168.1.56
Air6372S0 login: root
Password:

BusyBox v1.14.1 (2011-10-25 17:21:22 EEST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

# Built-in commands:
-----
. : [ alias bg break cd chdir continue echo eval exec exit export
false fg hash help jobs kill let local pwd read readonly return
set shift source test times trap true type ulimit umask unalias
unset wait
#
```

```
root@Batcave:/var/www/html/balkupu# cat balkupu.txt
29-12-2014 20:25|88.235.155.239|Username: root
29-12-2014 20:25|88.235.155.239|Password: SoL_FiBeR_1357
29-12-2014 20:25|88.235.155.239|Logged In!
29-12-2014 20:25|88.235.155.239|Command: help
29-12-2014 20:25|88.235.155.239|Command: ifcoifc
29-12-2014 20:25|88.235.155.239|Command:
29-12-2014 20:25|88.235.155.239|Command:
29-12-2014 20:25|88.235.155.239|Command:
29-12-2014 20:25|88.235.155.239|Command:
29-12-2014 20:25|88.235.155.239|Command:
29-12-2014 20:25|88.235.155.239|Command: help
10-01-2015 05:38|172.245.61.34|Username: root
10-01-2015 05:38|172.245.61.34|Password: dsl_2012_Air
10-01-2015 05:38|172.245.61.34|Logged In!
10-01-2015 05:38|172.245.61.34|Command: cat /var/hostapd*
10-01-2015 05:38|172.245.61.34|Command: ps
10-01-2015 05:38|172.245.61.34|Command: cat /var/config.xml
10-01-2015 05:38|172.245.61.34|Command: cat /etc/passwd
```



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 diskli 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

★★★★★
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 bedaval	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

Ana Sayfa > Bilgisayarlar > Bilgisayar Parçaları > Bellek Ramler > Kingston Bellek Ramler



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



Sandisk SSD Plus 120GB 520MB-180MB/s SATA3 2.5" SSD (SDSSDA-120G-G25)

%40 indirim **119,00 TL**

★★★★★
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 bedaval	Sepete Ekle
123,90 TL Cesur Bilişim	• En geç 10 Mayıs Salı günü kargoda • Bu mağazada kargo bedaval	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

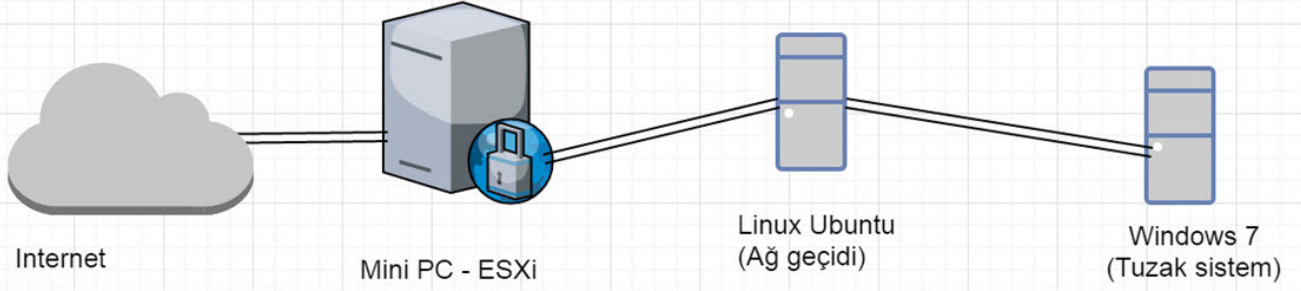
Name, Target or Status contains: Clear

Name	Target	Status	Details	Initiated by	Requested Start Time	Start Time	Completed Time
------	--------	--------	---------	--------------	----------------------	------------	----------------

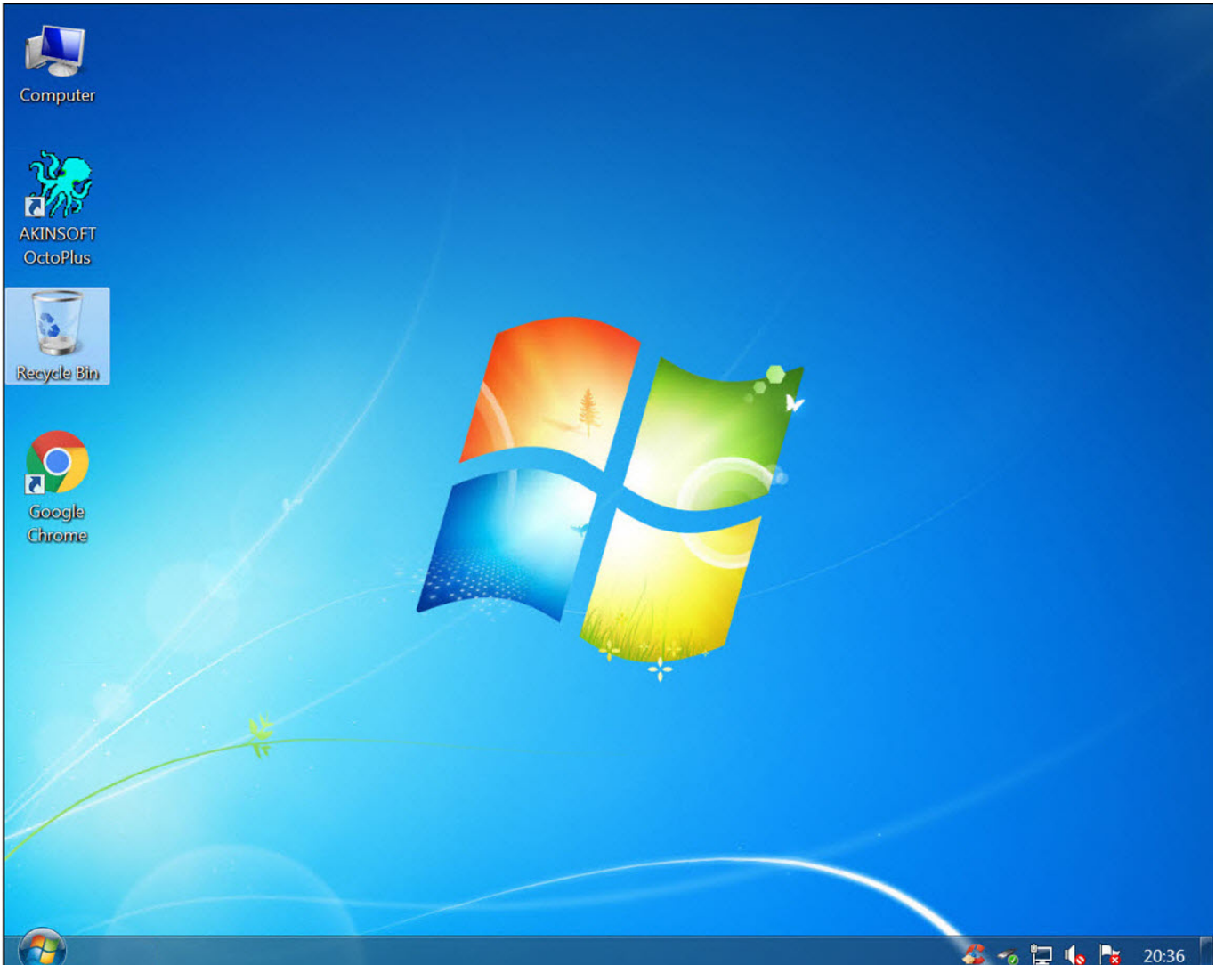
Tasks

To release cursor, press CTRL+ALT | root

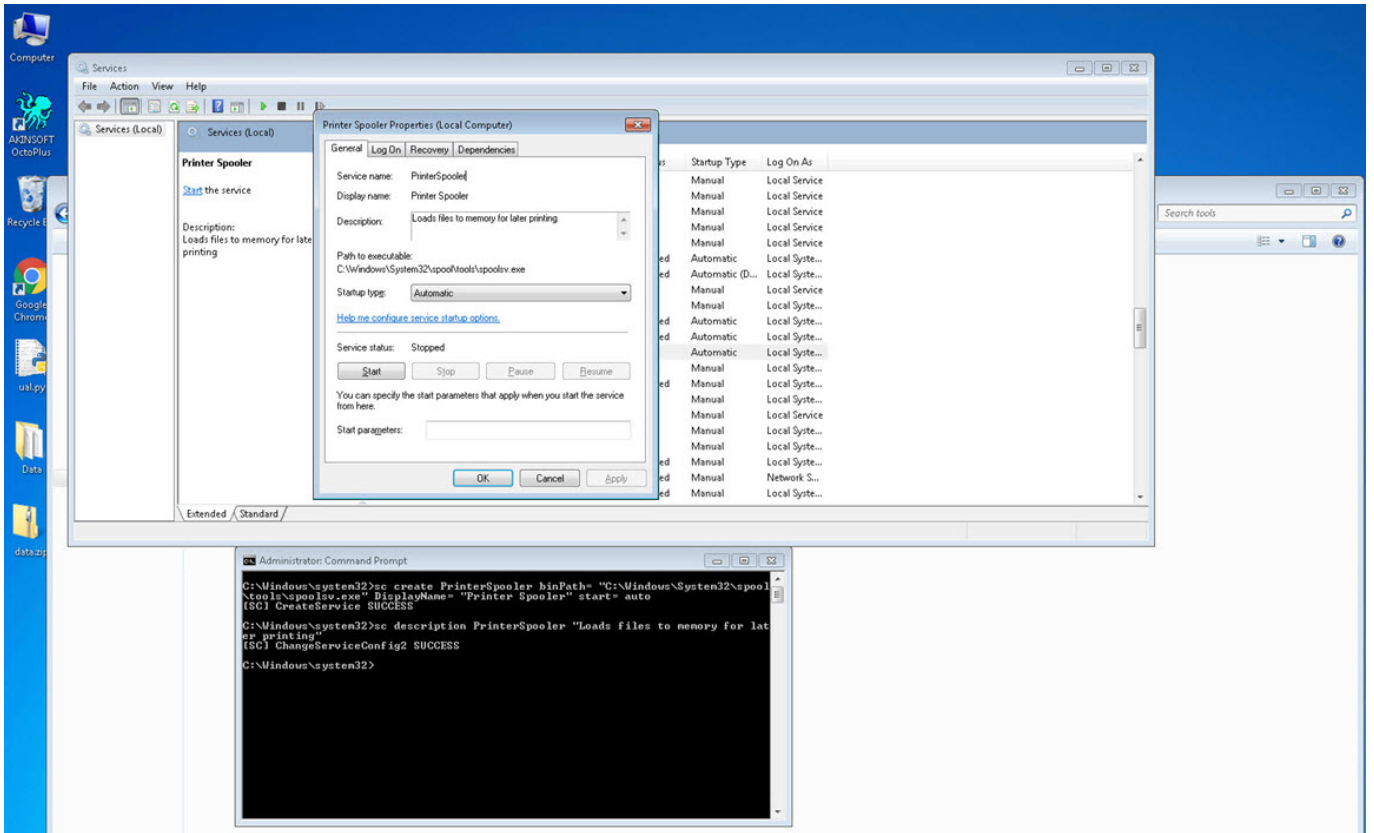
Tuzak Sistem Altyapısı



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 tercihim 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 başta 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

42 of about 86

←

Move to Inbox

More

User Activities

Inbox x

to me

Jun 22

★

data.zip

< data 6 items

keylogs.txt

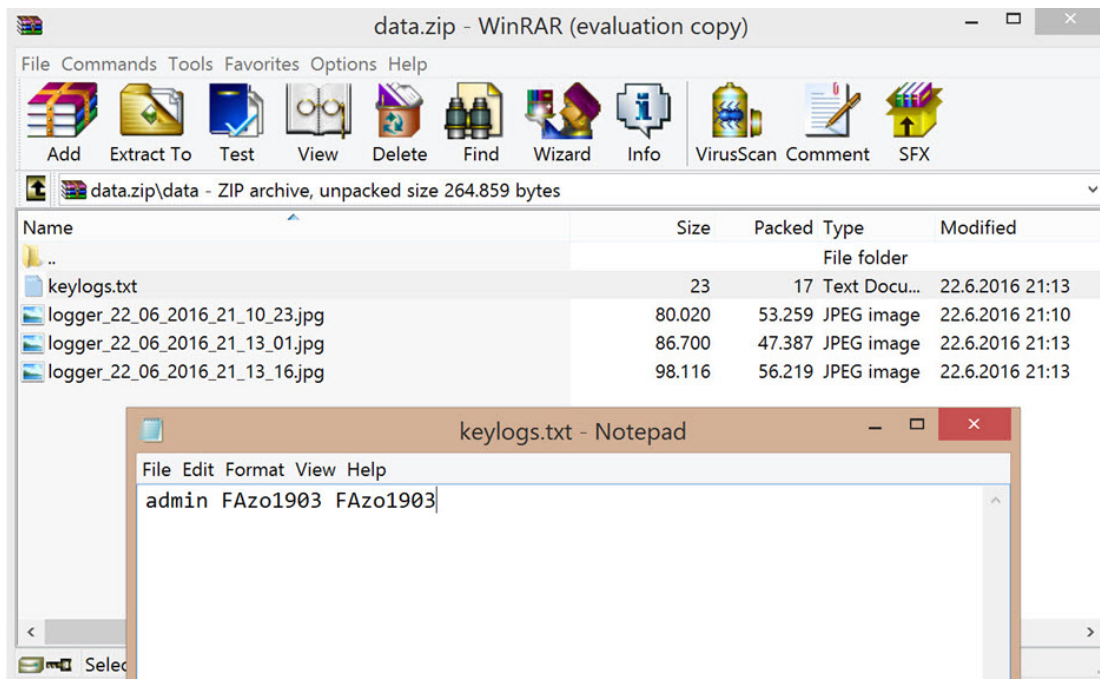
logger_22_06_2016_21_19_35.jpg

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



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

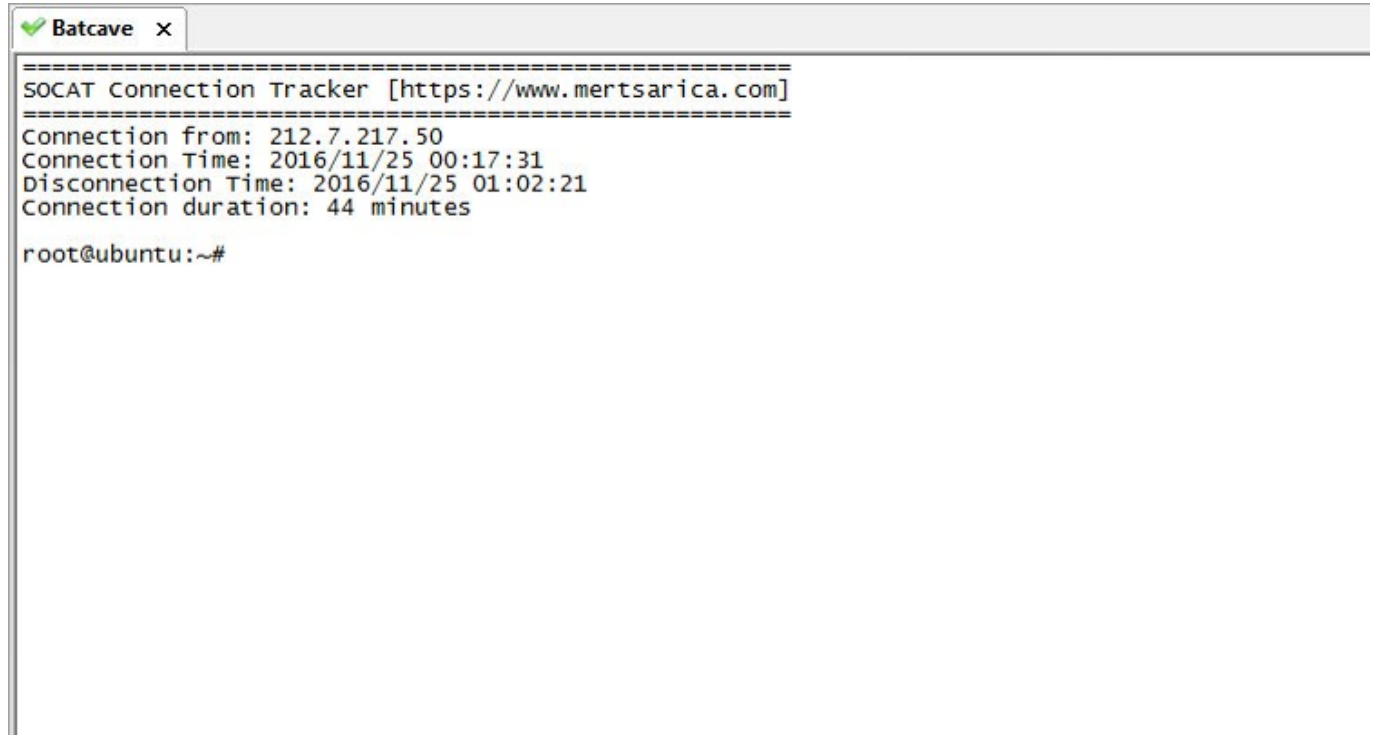
Polis 2011 yılından beri yaptığı araştırmada, incelenen 273 olayın 271'inde bir ize ulaşamadığı ancak 2 olayda yapılan hata sayesinde şebeke ele başı S.B.'ye ulaşıldı. Ukrayna'da yaşayan Türk vatandaşı bilgisayar mühendisi S.B.'nin 3 ay önce Türkiye'ye giriş yaptığı belirlendi. Polis S.B.'nin irtibatlarını 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.

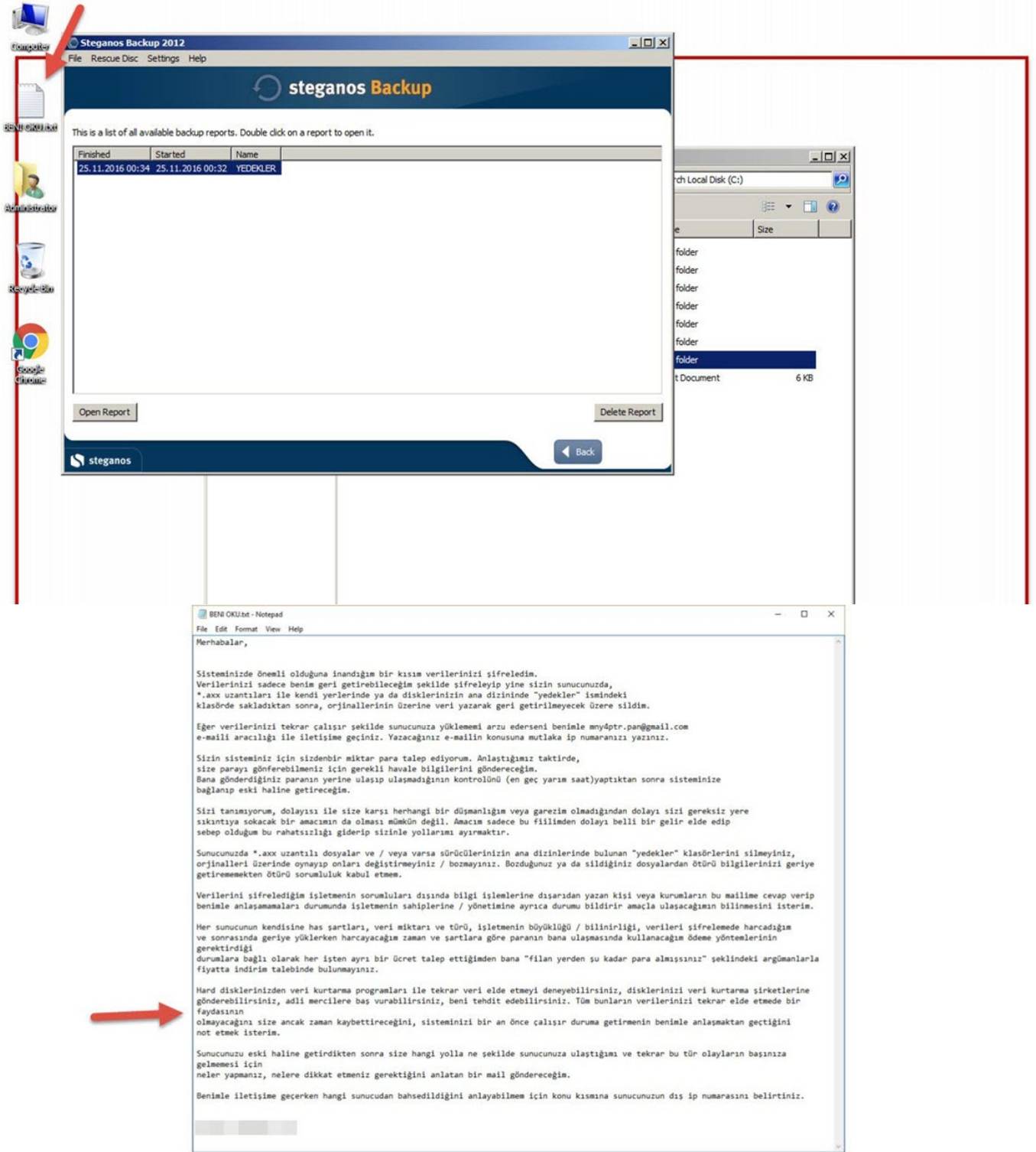
Tuzak sisteme bağlananların IP adreslerini ve sisteme ne kadar süre ile bağlı kaldıklarını öğrenebilme adına Remote Desktop servisine internetten erişim vermek yerine, Ubuntu (Batcave) üzerinden yönlendirme yapmaya karar verdim. Bunun için Ubuntu'nun 3389. bağlantı noktasına (port) gelen tüm istekleri, 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.



```
=====  
SOCAT Connection Tracker [https://www.mertsarica.com]  
=====  
Connection from: 212.7.217.50  
Connection Time: 2016/11/25 00:17:31  
Disconnection Time: 2016/11/25 01:02:21  
Connection duration: 44 minutes  
root@ubuntu:~#
```

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 oluşturulmuşuydu. 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.



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

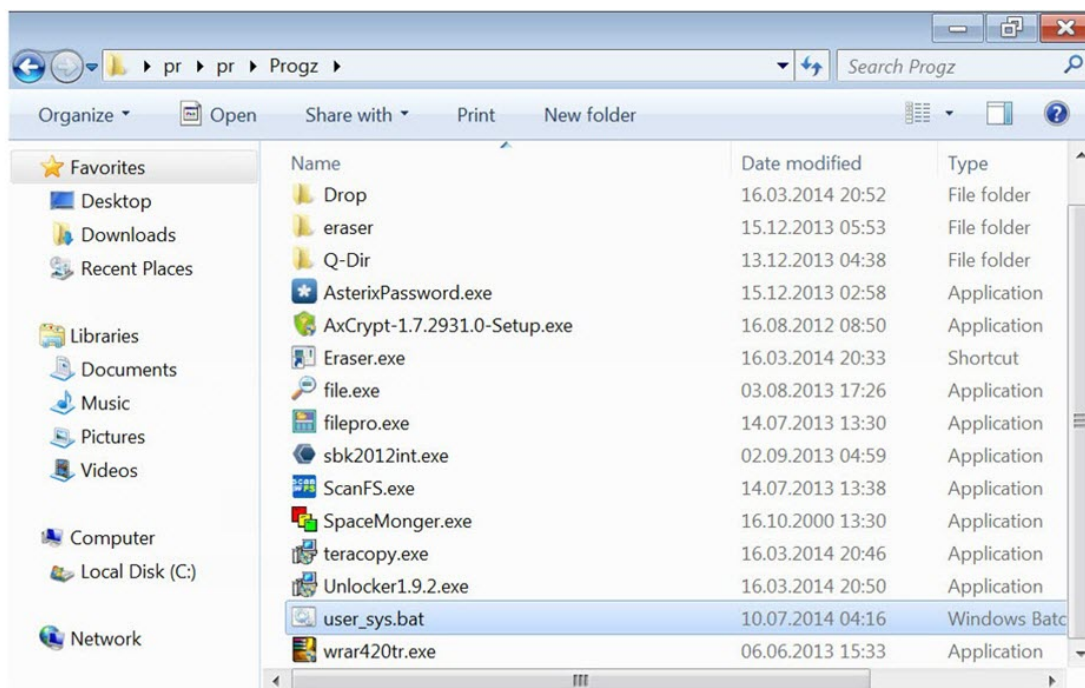
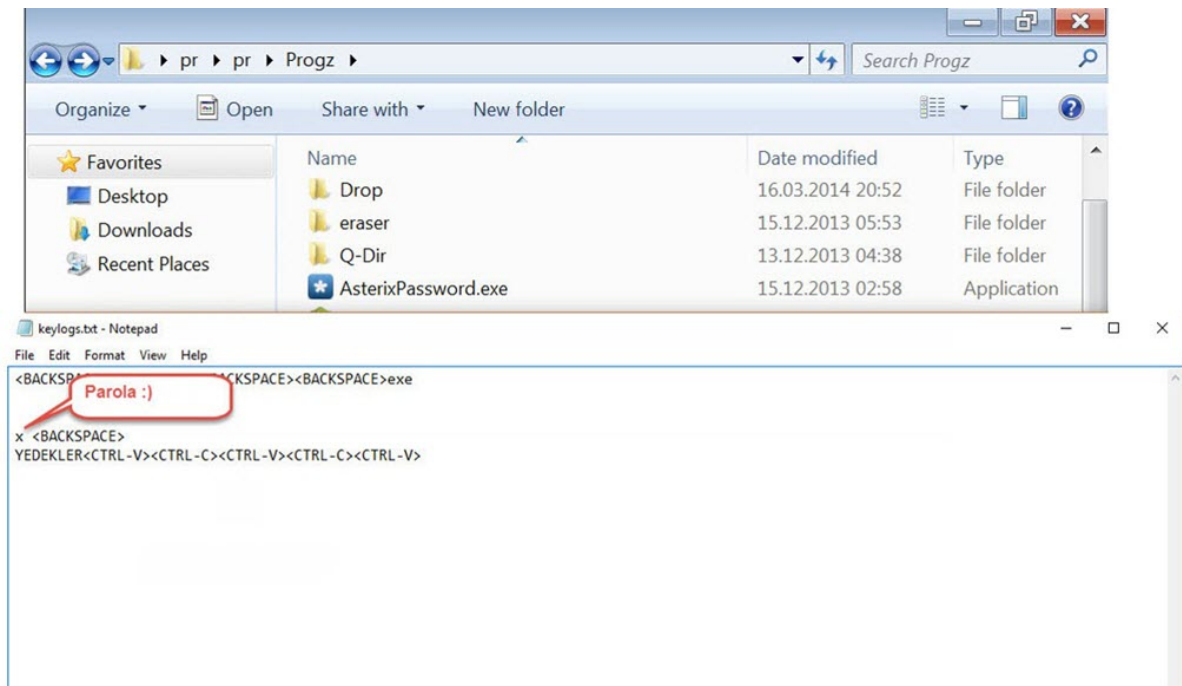
The screenshot shows a Windows File Explorer window with the address bar set to 'data > data'. The left sidebar shows the 'Quick access' menu with 'Desktop', 'Downloads', 'Dropbox', 'Pictures', and 'Documents' listed. The main pane displays a grid of files. The first file is 'keylogs.txt', which is selected. Below it are several image files with names like 'logger_25_11_201_6,00_17_51.jpg'. A Notepad window is open in the foreground, titled 'keylogs.txt - Notepad'. The text in the Notepad window is a long string of characters, including file names and a URL: '<CTRL-V><CTRL-V>www.kameder.com.tr/dokumanlar/pr.docx'. A red arrow points to the end of this string.

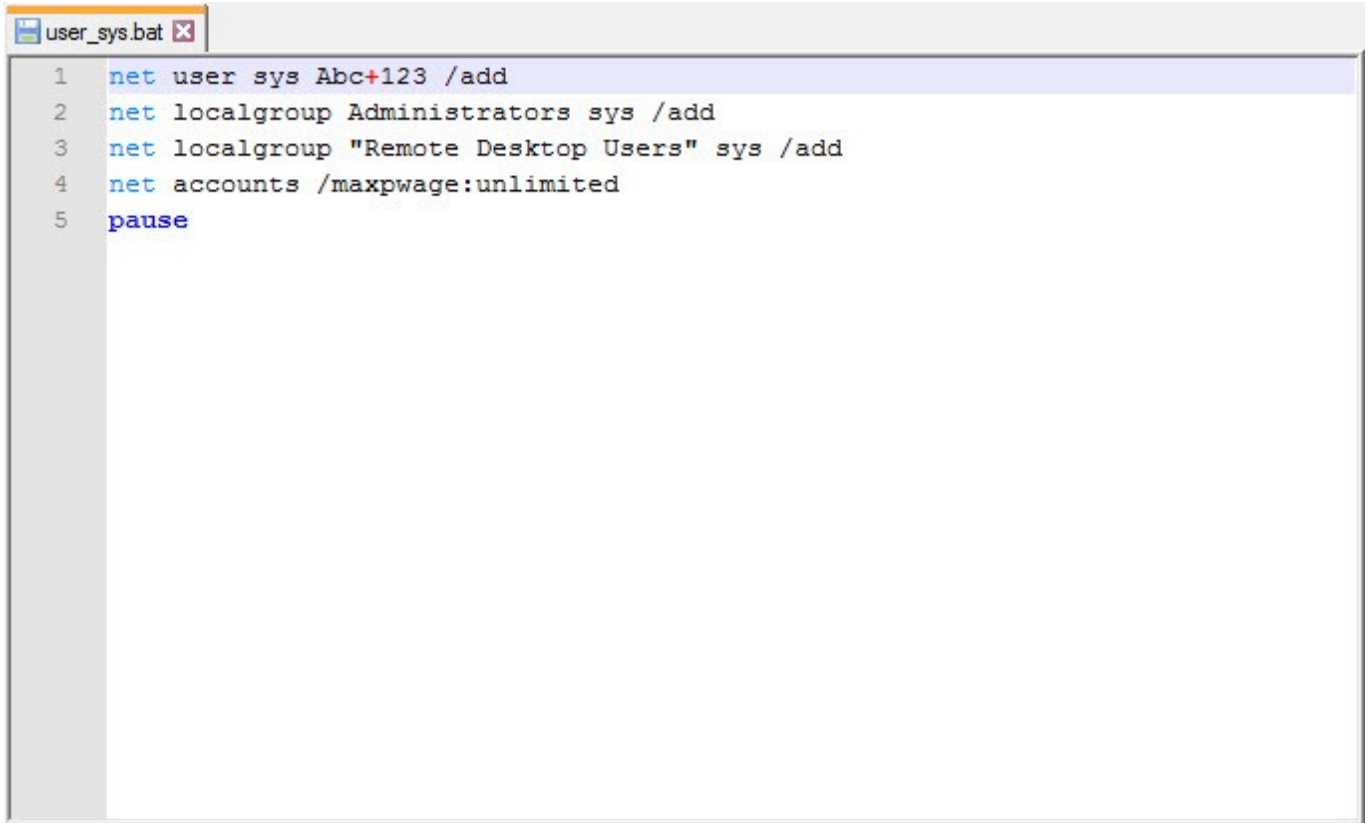
```

root@remnux: /home/remnux/Desktop/honeypot
File Edit Tabs Help
root@remnux:/# cd home
root@remnux:/home# ls
remnux
root@remnux:/home# cd remnux/
root@remnux:/home/remnux# cd Desktop/
root@remnux:/home/remnux/Desktop# mkdir honeypot
root@remnux:/home/remnux/Desktop# cd honeypot/
root@remnux:/home/remnux/Desktop/honeypot# wget www.kameder.com.tr/dokumanlar/pr.docx
--2016-11-24 21:54:31-- http://www.kameder.com.tr/dokumanlar/pr.docx
Resolving www.kameder.com.tr (www.kameder.com.tr)... 77.223.129.229
Connecting to www.kameder.com.tr (www.kameder.com.tr)|77.223.129.229|:80...
ected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://kameder.com.tr/dokumanlar/pr.docx [following]
--2016-11-24 21:54:32-- http://kameder.com.tr/dokumanlar/pr.docx
Resolving kameder.com.tr (kameder.com.tr)... 77.223.129.229
Reusing existing connection to www.kameder.com.tr:80.
HTTP request sent, awaiting response... 200 OK
Length: 68230834 (65M) [application/vnd.openxmlformats-officedocument.wordprocessingml.document]
Saving to: 'pr.docx'

pr.docx          42%[=====>] 27.76M  1.51MB/s  eta 1

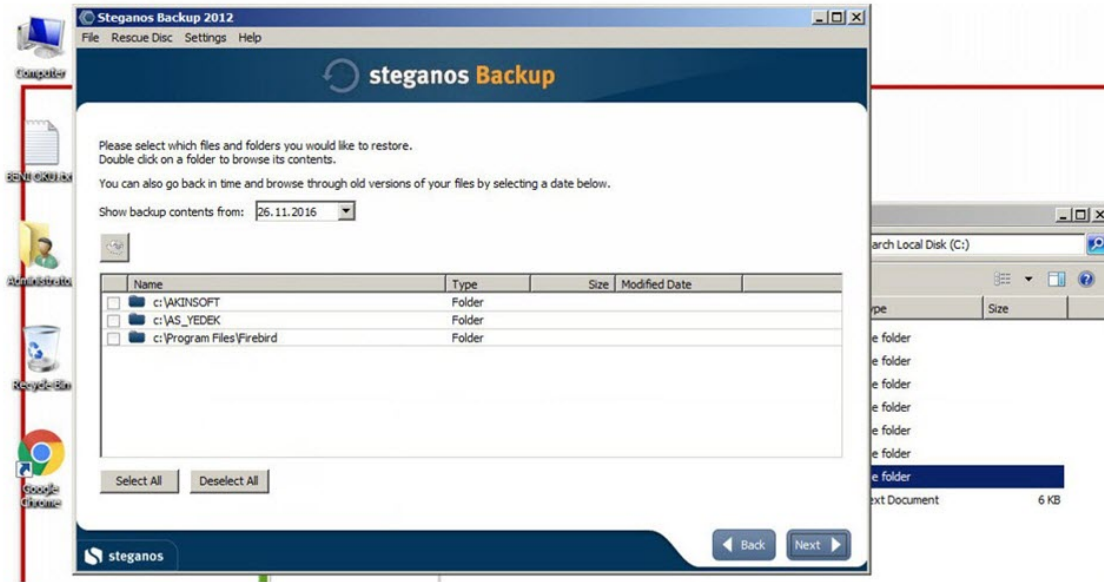
```





```
1 net user sys Abc+123 /add
2 net localgroup Administrators sys /add
3 net localgroup "Remote Desktop Users" sys /add
4 net accounts /maxpwage:unlimited
5 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 başlayan bir parola denemiş ve onu da yazamayınca 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.



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.