

Hacker Hunt with a Deception System

written by Mert SARICA | 3 July 2017

I have been hearing this question more and more frequently from many people around me, both those I know and those I don't know, in recent years: "My data has been encrypted, they're asking for money, what can I do? Who can I get help from?" I see this as similar to the question, "I lost my arm, what can I do?" from someone who didn't put on their seatbelt and then smashed into a wall at high speed. Unfortunately, some mistakes are not easily or even possible to fix. In the cyber world where encryption malware is running rampant, if you don't regularly back up your data, use strong passwords on your systems/devices (such as using a combination of upper and lowercase letters and special characters), and harden the security of your systems, it won't be long before you inevitably become the target of someone's malicious intent, directly or indirectly. If you look at the security research I've done from the past to the present, you'll be able to understand what I mean better.



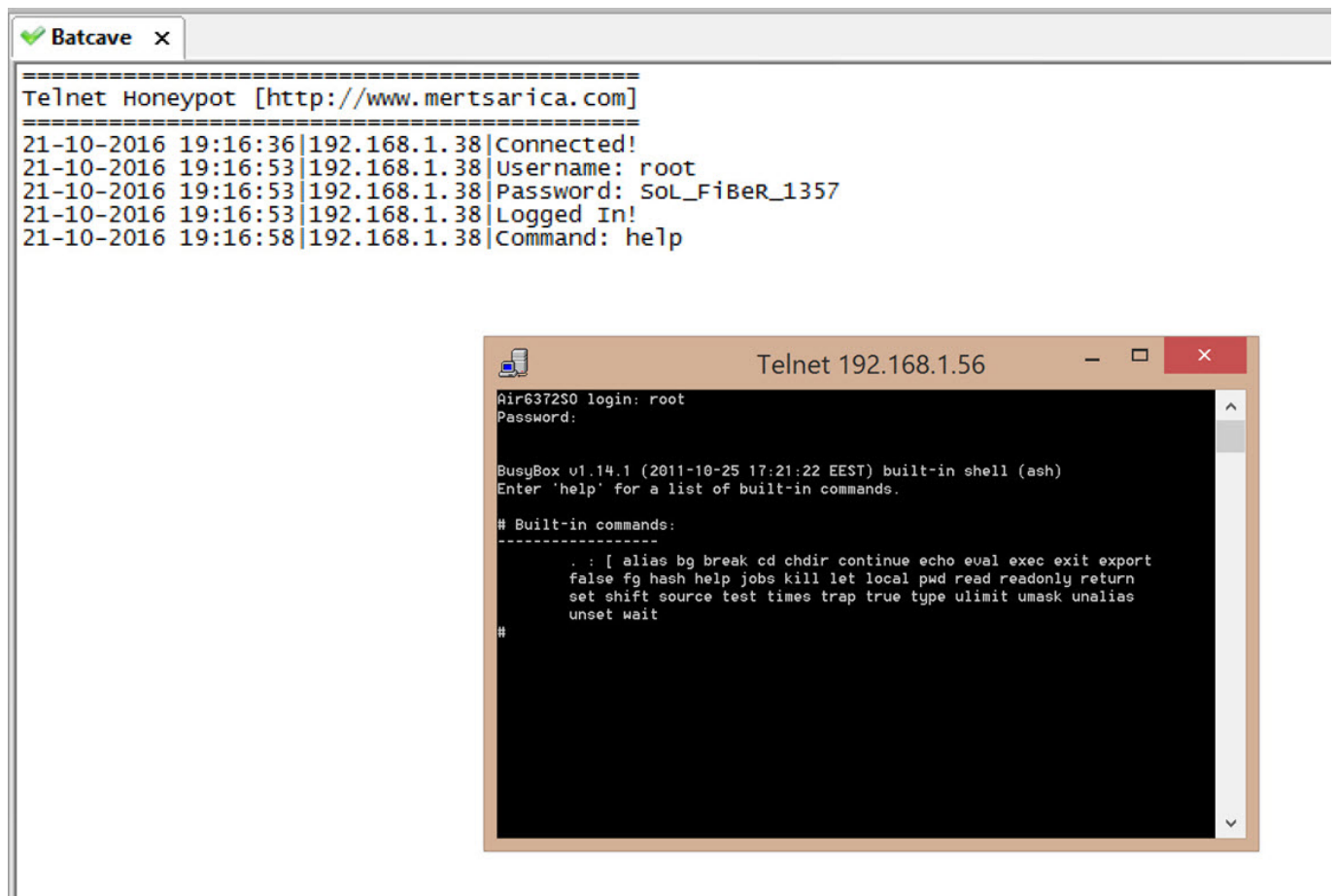
Mert bey merhaba, 2 gün önce başımız geldi, 2 ay öncede İstanbuldaki bir firmaya. Müşteride tüm veritabanlarını ve ortak kullannılan dosyaları şifrediler ve para istiyorlar. Bu konuda 3389 portu haricinde yapılabilecekler, alınması gereken önlemler konusunda yardımcı olabilmisiniz. Vatandaşlar Active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

In my blog post "Virtual Siege" that I wrote in 2010, I set up a simple honeypot at my home, and the point I was trying to make with the following sentence was that the problems faced by end users today in the virtual world were almost like echoes of what I had highlighted in the post.

"If I were to briefly summarize the information I obtained from the honeypot records, I would say that the first connection was made to one of the 11 ports on the honeypot within 12 minutes of being connected to the internet, and in the next 5 hours, a total of 14 different IP addresses from 8

different countries had established communication with the honeypot.”

In another blog post of mine titled “Air6372S0 Default Account Verification” in 2014, I tried to draw attention to how user names and passwords embedded in hardware and software can endanger our security as end-users. In the post, I also quietly put into action a fake Telnet Honeypot tool that I had designed to accept incoming connections, which would impersonate itself as the console interface of an Airties modem. The tool would record anyone trying to connect using the embedded passwords that were the subject of the post. After the post was published, a short time later I found that it was receiving connections from both inside and outside of the country. One of those connections came from an IP address in England (172.245.61.34) that had successfully intercepted the name and password of a WiFi access point and was trying to crack the password. When I thought about the reason behind this, it was likely that malicious individuals could be building dictionaries of passwords or could use this information to commit cyber crimes through your WiFi modem.



The image shows two terminal windows. The top window, titled 'Baticave', displays a log of Telnet Honeypot activity. The log shows a connection from 192.168.1.38 at 19:16:36, followed by a successful login with the username 'root' and password 'SoL_FiBeR_1357'. The user then enters the command 'help'. The bottom window, titled 'Telnet 192.168.1.56', shows the user's perspective of the Telnet session. It displays the login prompt, the user's input of 'root' and 'Password:', and the resulting BusyBox shell prompt. The shell prompt shows the version of BusyBox and a list of built-in commands.

```
=====
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
```



Towards the end of 2016, I decided to shed light on the methods used by ransomware attackers who were using the encryption method I mentioned in the beginning of the post. According to rumors, malicious individuals were scanning Turkish IP blocks with tools such as Nmap, targeting open Remote Desktop services and performing dictionary attacks using tools such as Ncrack. I began collecting the necessary hardware for this research without breaking my budget (in 6 installments).

After collecting the hardware, I ended up with a deception system that had a 2GHz processor, 8GB of RAM, and a 120GB SSD disk. So first, I installed the free ESXi virtualization system, and on top of that, I installed a Windows 7 (Honeypot) with a fake accounting application to catch malicious individuals who hack the trap system, and to monitor the network traffic and limit internet connection. I also installed an Ubuntu operating system (Batcave) to make sure that the system can't be used for other crimes. I isolated Windows 7 on the local network and used Ubuntu as a proxy server (with ssl inspection) to connect to the internet.



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)

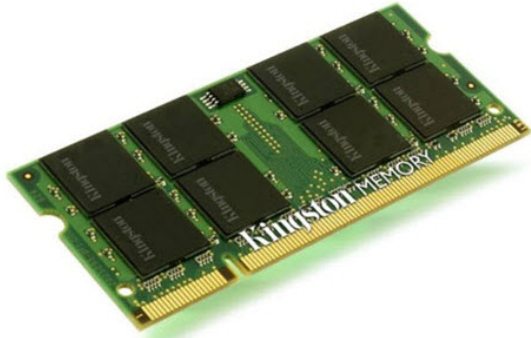
Taksit

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

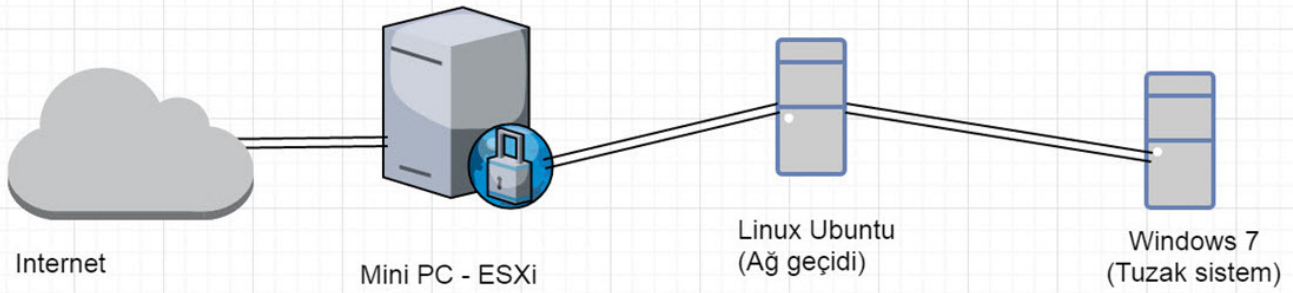
Name, Target or Status contains: Clear

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

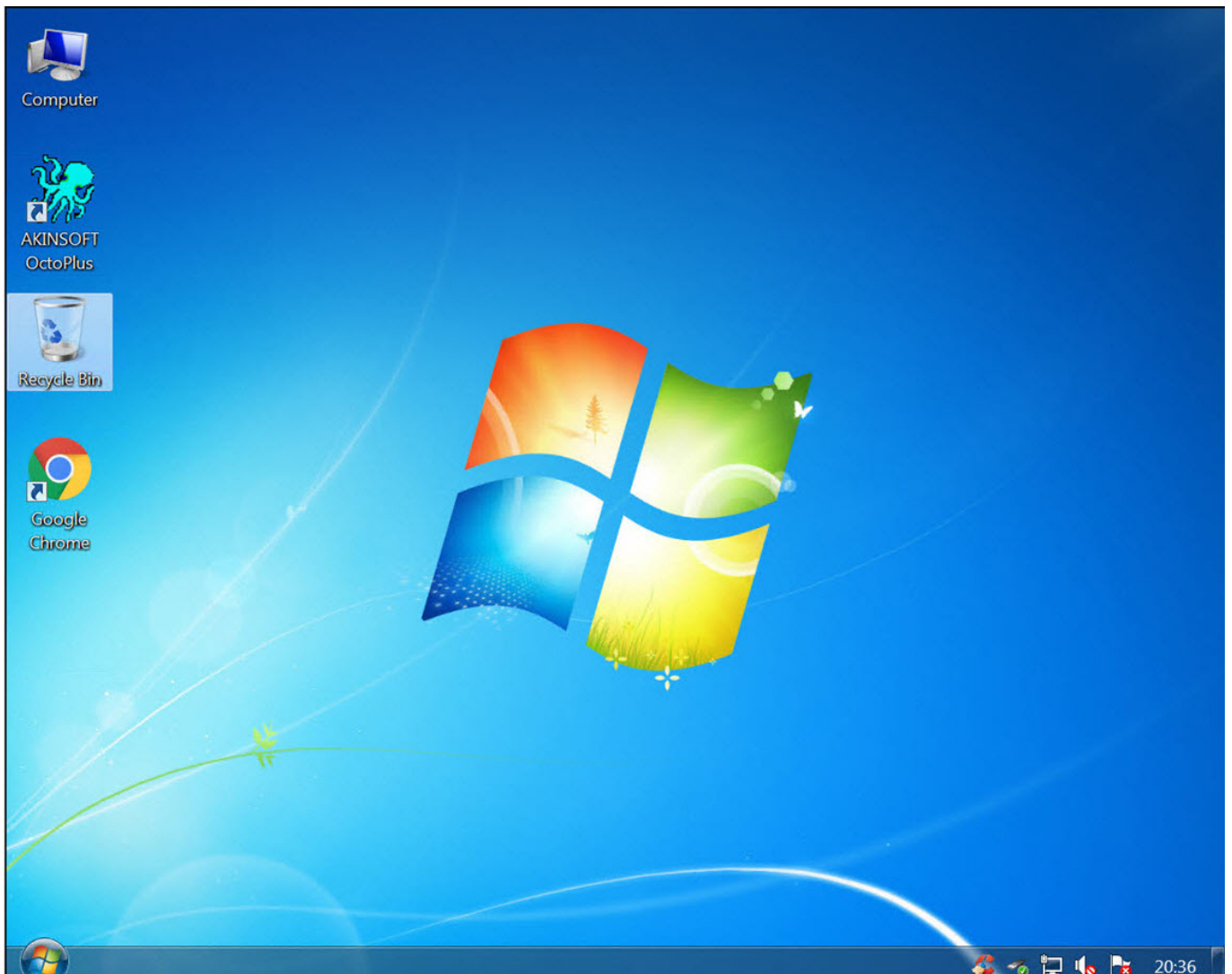
Tasks

To release cursor, press CTRL+ALT | root

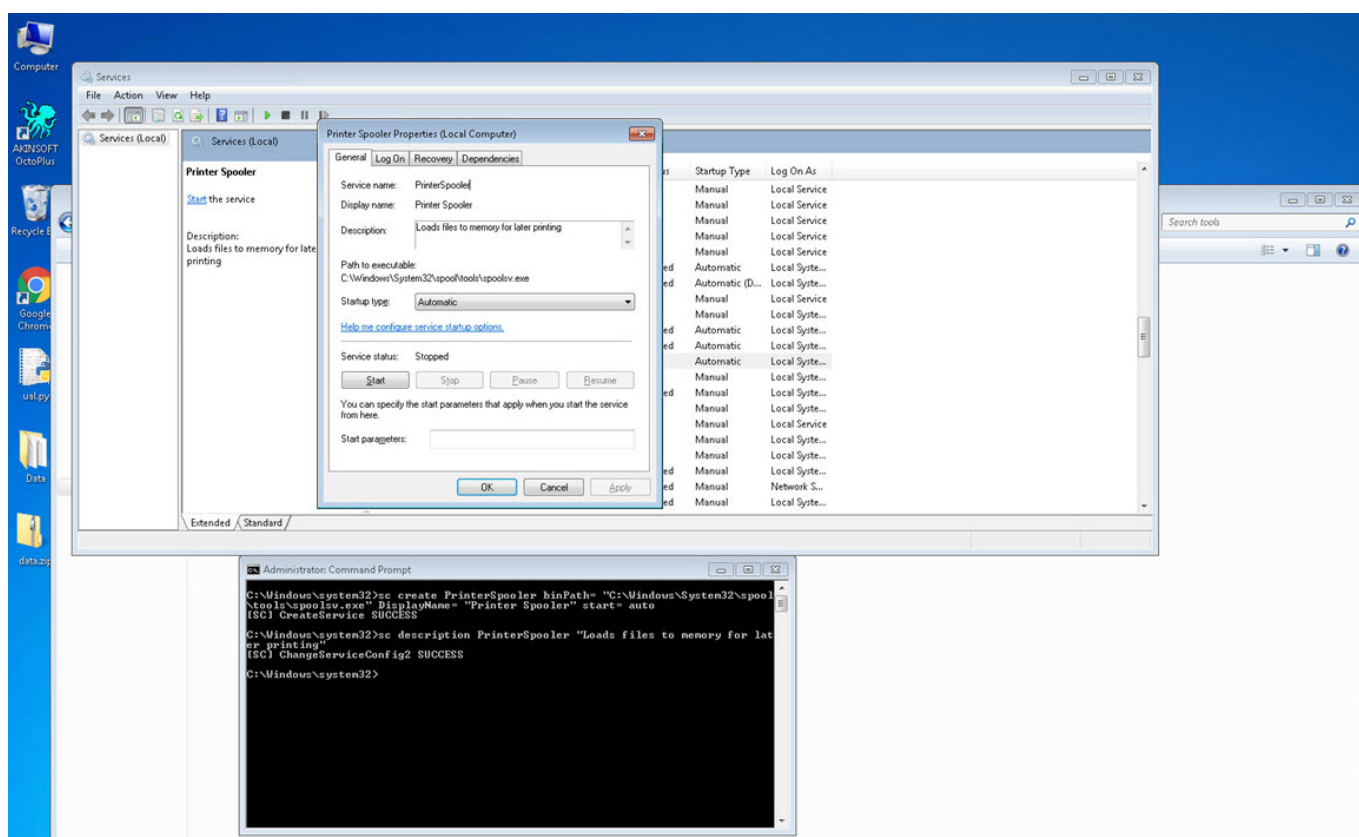
Tuzak Sistem Altyapısı



To make the deception system more attractive to malicious individuals, I began searching for an accounting software to install on the Windows 7-based system. To decide which accounting software to use, I used information I had gathered from victims of data encryption and chose Akinsoft's OctoPlus software.

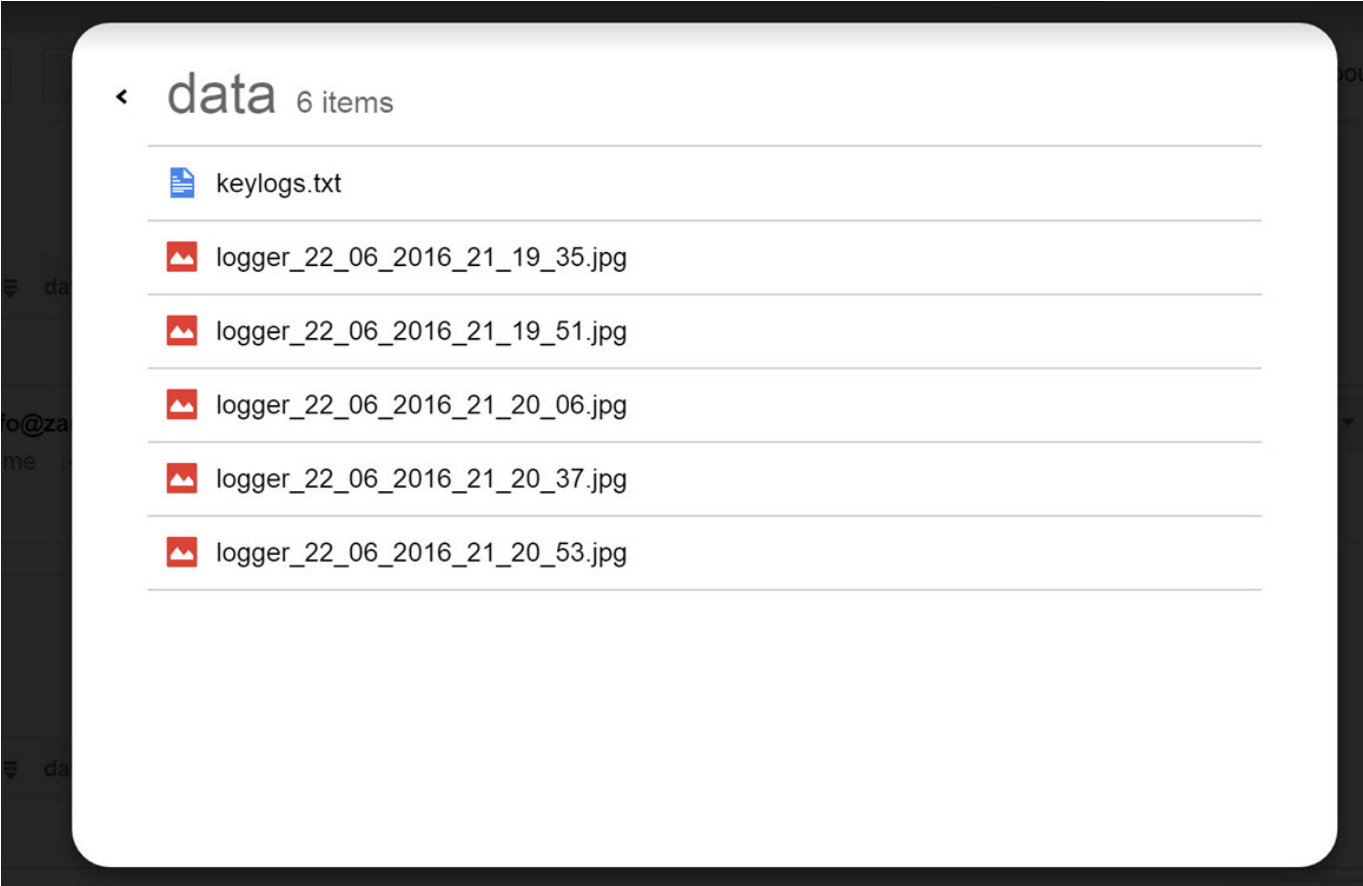
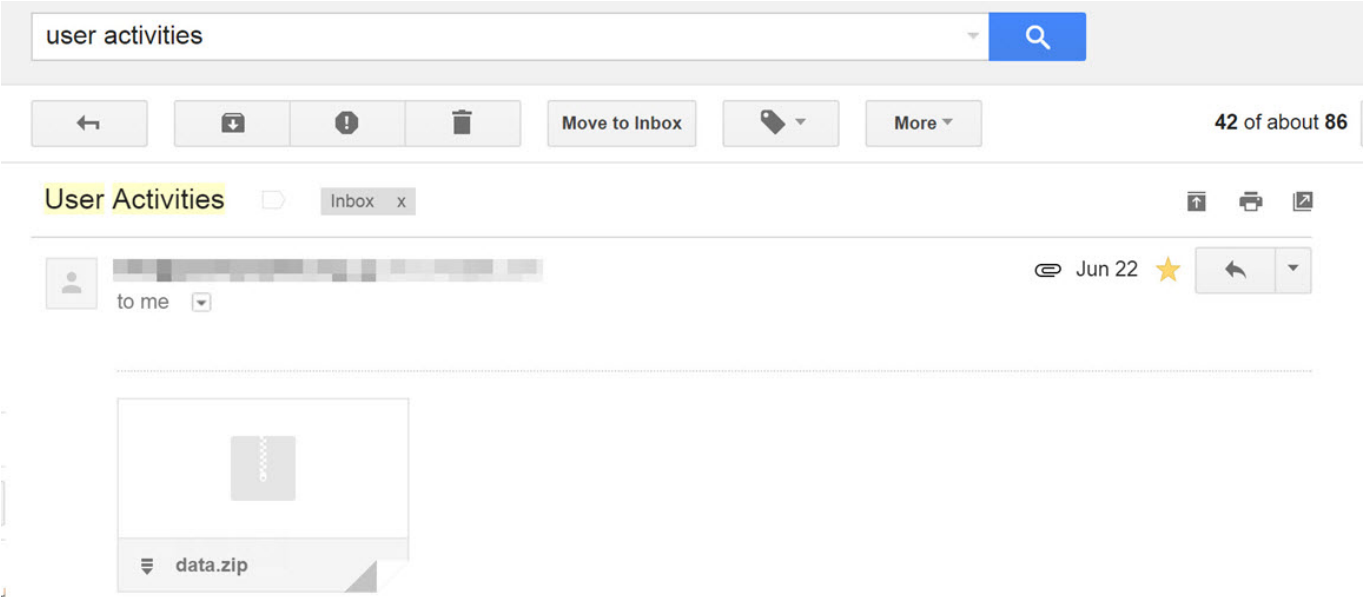


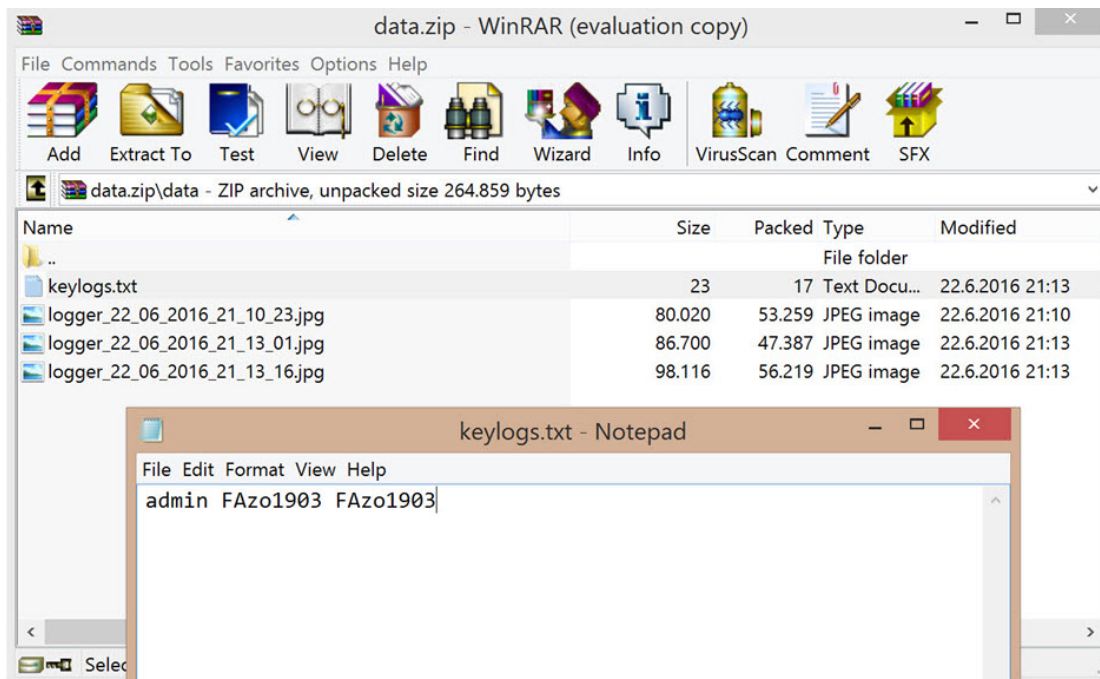
When it came time to design the tool that would make the deception system a trap, I created a tool called UAL (User Activity Logger) using Python. It would record all of the user's actions on Windows (keystroke logging, video recording, screen capture, clipboard copying) and sends all information except the video file every 5 minutes by email. However I decided not to share the source code for this tool for the safe use of it. To avoid raising the suspicions of the malicious individuals who connect to the trap system, I hid various folders, including the Python27 folder, on the operating system. Then, I changed the name of the compiled UAL.py tool to spoolsv.exe, and registered it as a Windows service so that it would run again with each session.



After setting up the deception system, with an admin password called accounting, and allowing access to the internet through the modem, I began monitoring the system for 6 months. During this time, I made many improvements to the system thanks to the information obtained from those who fell into the trap. For example, many malicious individuals checked the modification date of files before encrypting them to see if the accounting program was actively being used. Although some were able to crack the administrator password of the trap system using dictionary attacks, it took nearly 6 months for one of the ransomware attackers, who targeted individuals and made the news, encrypting data and leaving a note, to fall

into the deception system.





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

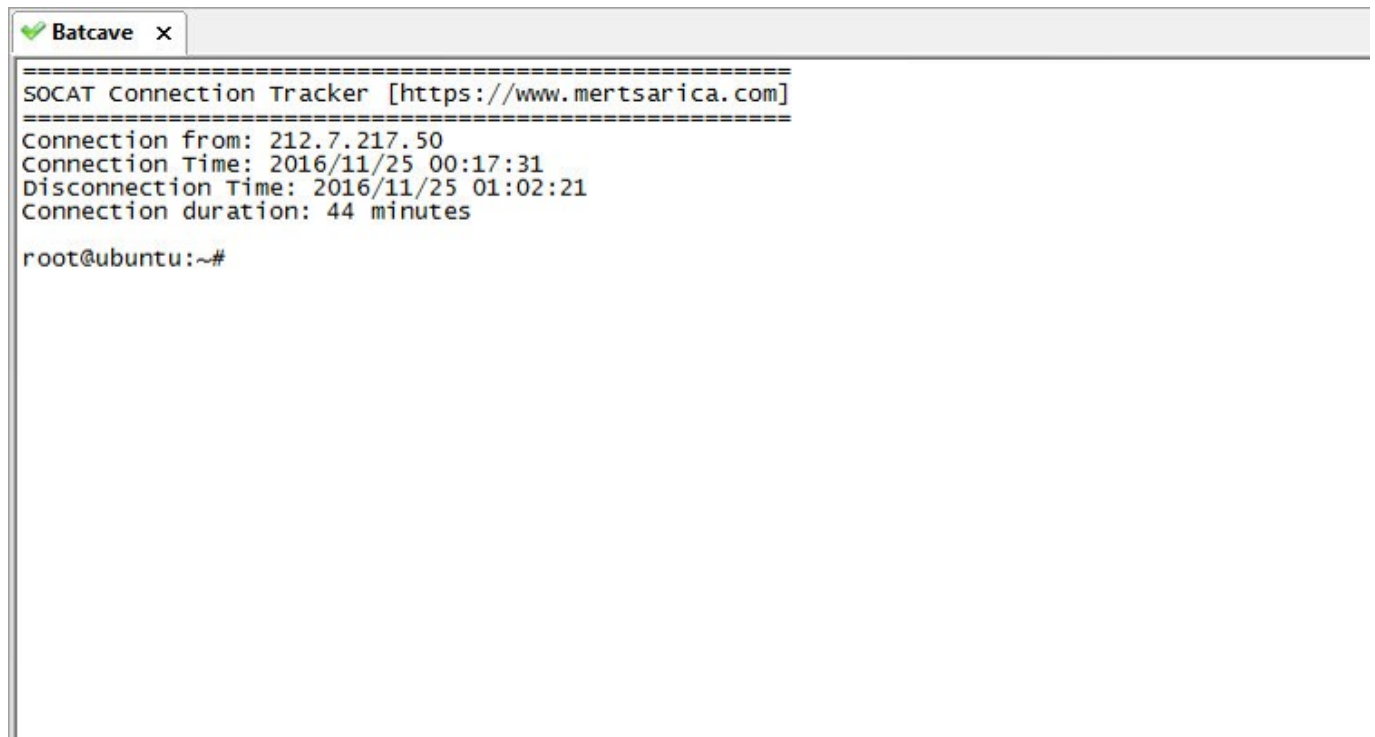
Polis 2011 yılından beri yaptığı araştırmada, incelenen 273 olayın 271'inde bir ize ulaşamadığı ancak 2 olayda yapılan hata sayesinde şebeke ele başı S.B.'ye ulaşıldı. Ukrayna'da yaşayan Türk vatandaşı bilgisayar mühendisi S.B.'nin 3 ay önce Türkiye'ye giriş yaptığı belirlendi. Polis S.B.'nin irtibatlarını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

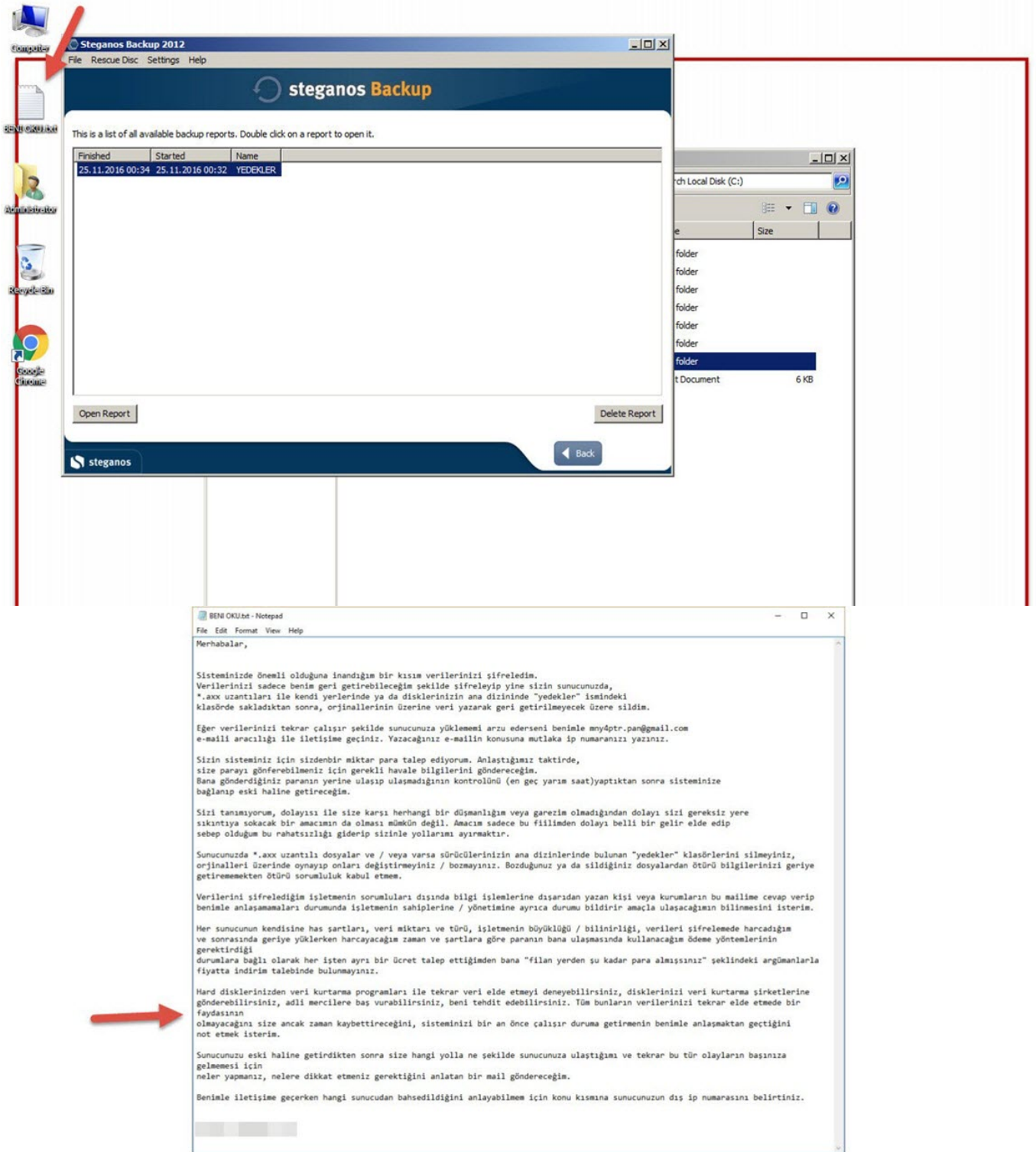
To be able to know the IP addresses of those who connect to the trap system and how long they stayed connected, I decided to redirect connections through Ubuntu (Battcave) instead of allowing internet access to the Remote Desktop service. To do this, I used the socat tool on Ubuntu to redirect all requests to port 3389 to the trap system's port 3389. Since the detailed logging feature of socat was not practical to read, I also created an additional tool

in Python called Socat Connection Tracker to help in monitoring connections.



```
✓ Batcave x
=====
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:~#
```

One morning, I woke up and found that my email inbox had received many emails sent by the deception system, indicating that someone had hacked the system while I was asleep. When I connected to the trap system's console through the ESXi interface, the first thing that caught my attention was that a new user named 'Sys' had been created. When I logged in, I saw that the accounting program's folders were encrypted and backed up with Steganos Backup 2012 software and there was a note on the desktop. It became clear that the day I had been waiting for had finally come and the connection was made by someone stayed connected for 44 minutes which can be seen from the screenshot provided.



Upon reviewing the records of the malicious person, I found that he had downloaded a file named "pr.docx" from a website (likely a hacked one) called kameder.com.tr. Because the file was a 65 MB document, it seemed suspicious and I was able to find out that it was a ZIP file. When I tried to open the ZIP file, it asked for a password. Quickly checking the records, I found that the password was x. Upon opening the ZIP file, I found all the tools that the malicious person had used to upload and run on the hacked system. After

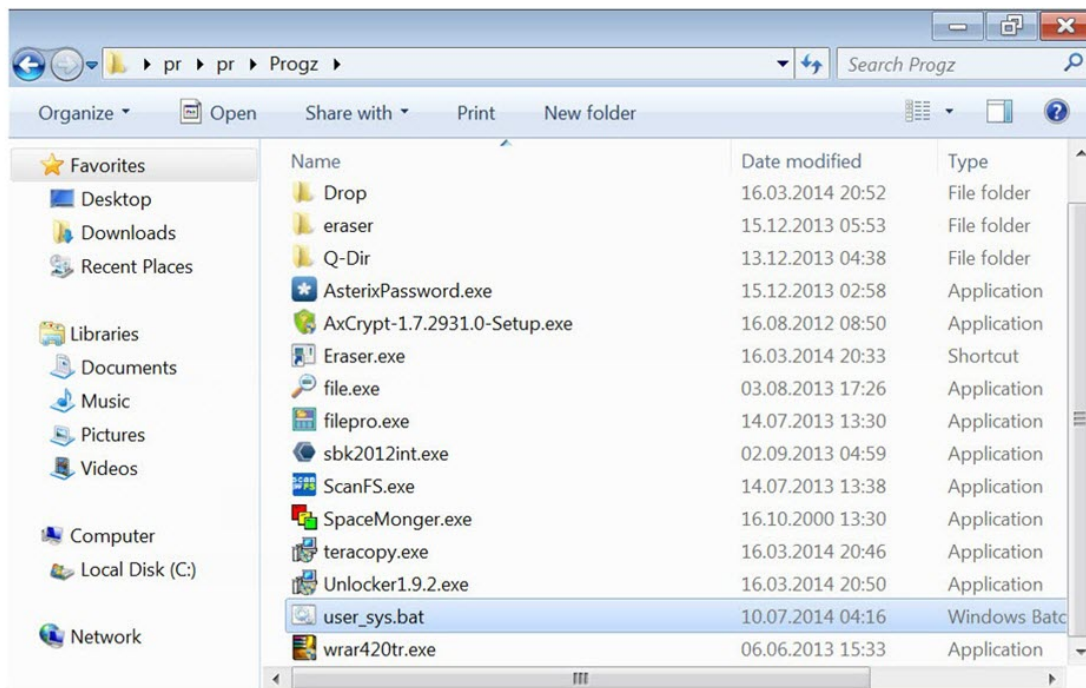
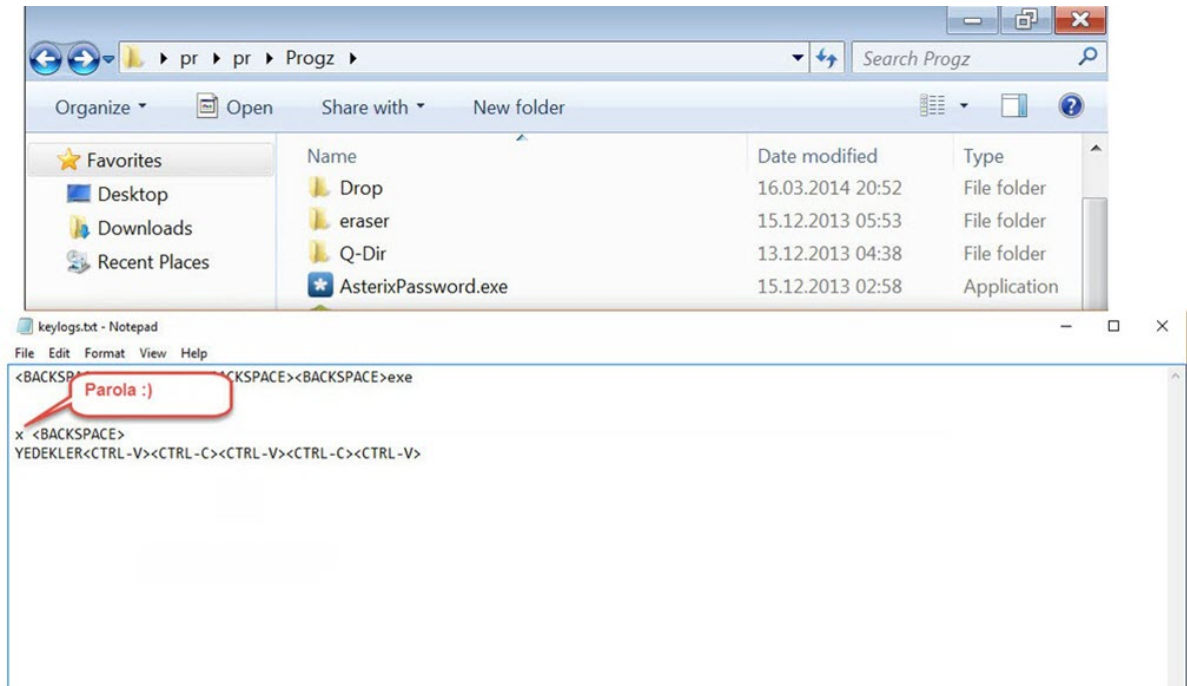
The screenshot shows a Windows File Explorer window with the address bar set to 'data > data'. The left sidebar shows the 'Quick access' menu with 'Desktop', 'Downloads', 'Dropbox', 'Pictures', and 'Documents' listed. The main pane displays a grid of files. The first file is 'keylogs.txt', which is selected. Below it are several files named 'logger_25_11_201' followed by timestamps in 'dd_mm_yy.jpg' format. A Notepad window titled 'keylogs.txt - Notepad' is open in the foreground, showing the contents of the selected file. The text in the Notepad window is a list of file names, mostly starting with '<CTRL-V>', followed by a URL: 'www.kameder.com.tr/dokumanlar/pr.docx'. A red arrow points to this URL.

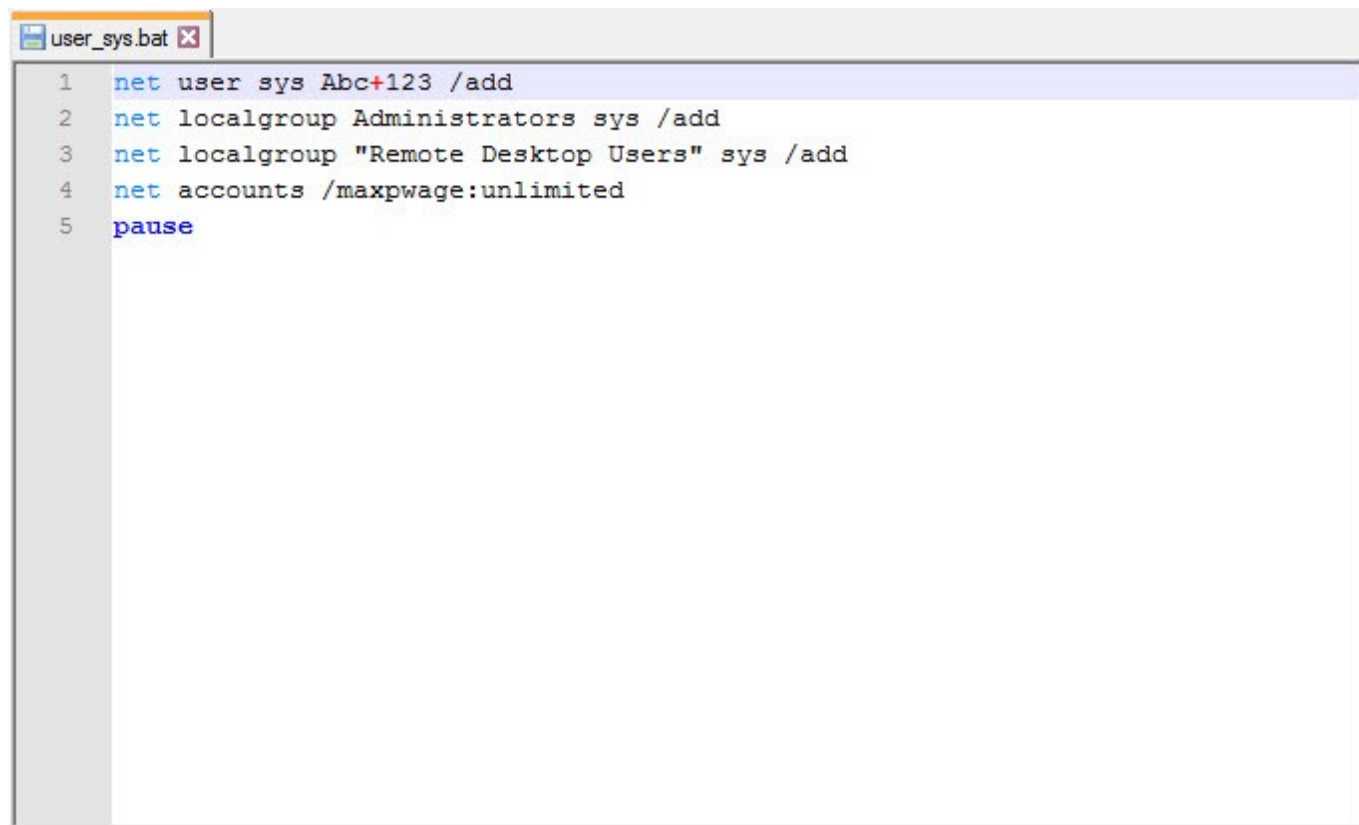
```

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:

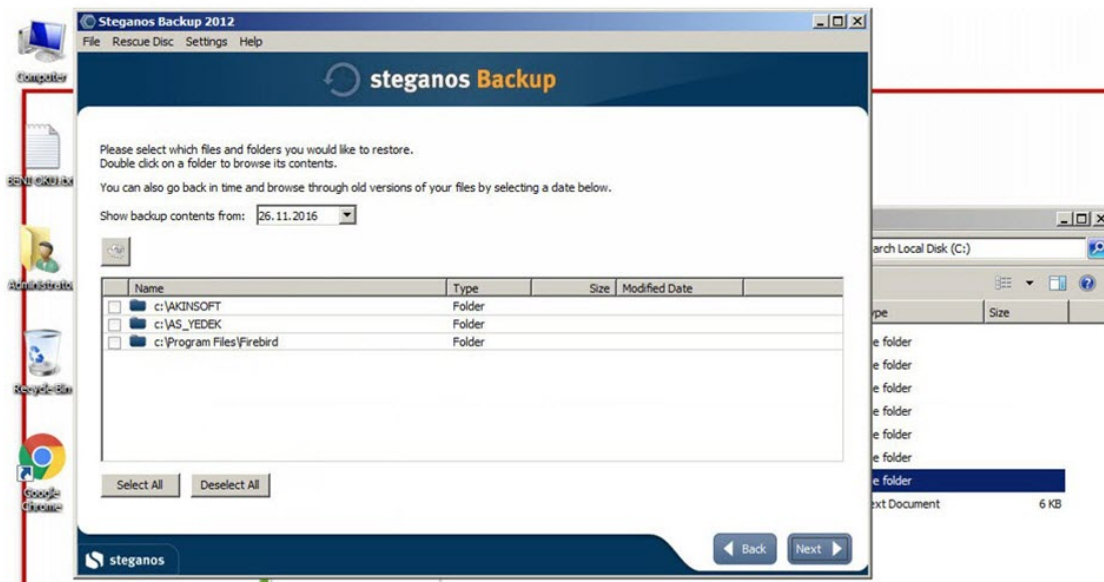
```





```
1 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
```

I noticed that the malicious person had a hard time typing in the password they had chosen to encrypt the accounting program's folders due to the trap system copy-pasting and blocking file sharing. :) After struggling to type in the long password starting with SEMSIPASA, they had tried a password starting with KARSIYAKA and failed to type it in, and had finally decided on the password of DVDASSANAT669-. Without knowing they were being monitored, the malicious person had planned to encrypt the data and send it via email, but thanks to the deception system, I was able to decrypt the password with DVDASSANAT669- and clarify the situation for myself.



In conclusion, in order to combat ransomware, it is important to periodically backup your systems, store your backups in a secure location, check and disable unnecessary internet connections, and use strong passwords on your systems. This will make it more difficult for ransomware to achieve its nefarious goals in the short term.

Additionally, you can watch the video that the trap system recorded of the malicious person encrypting the data in the link below.

Hope to see you in the following articles.