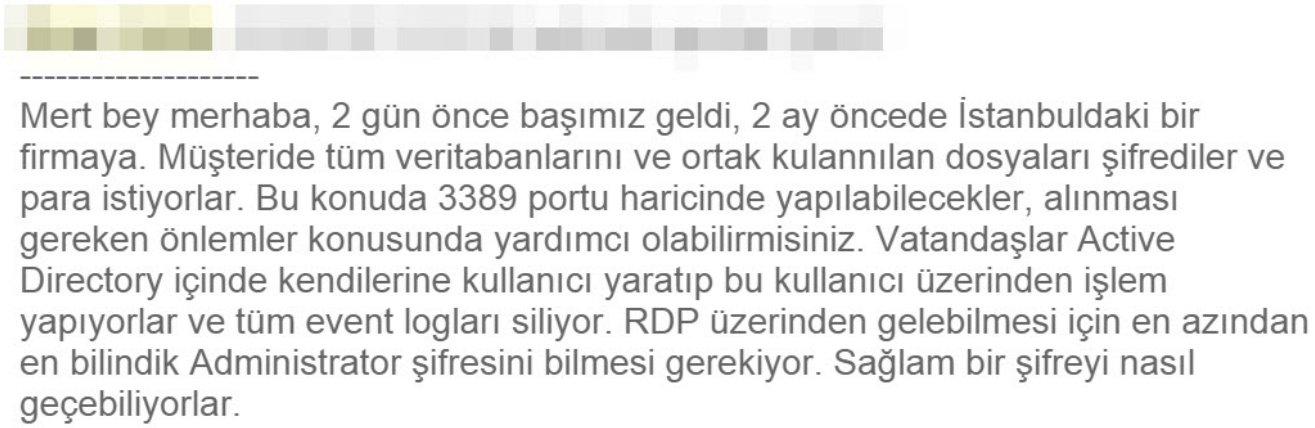
Hacker Hunt with a Deception System

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.



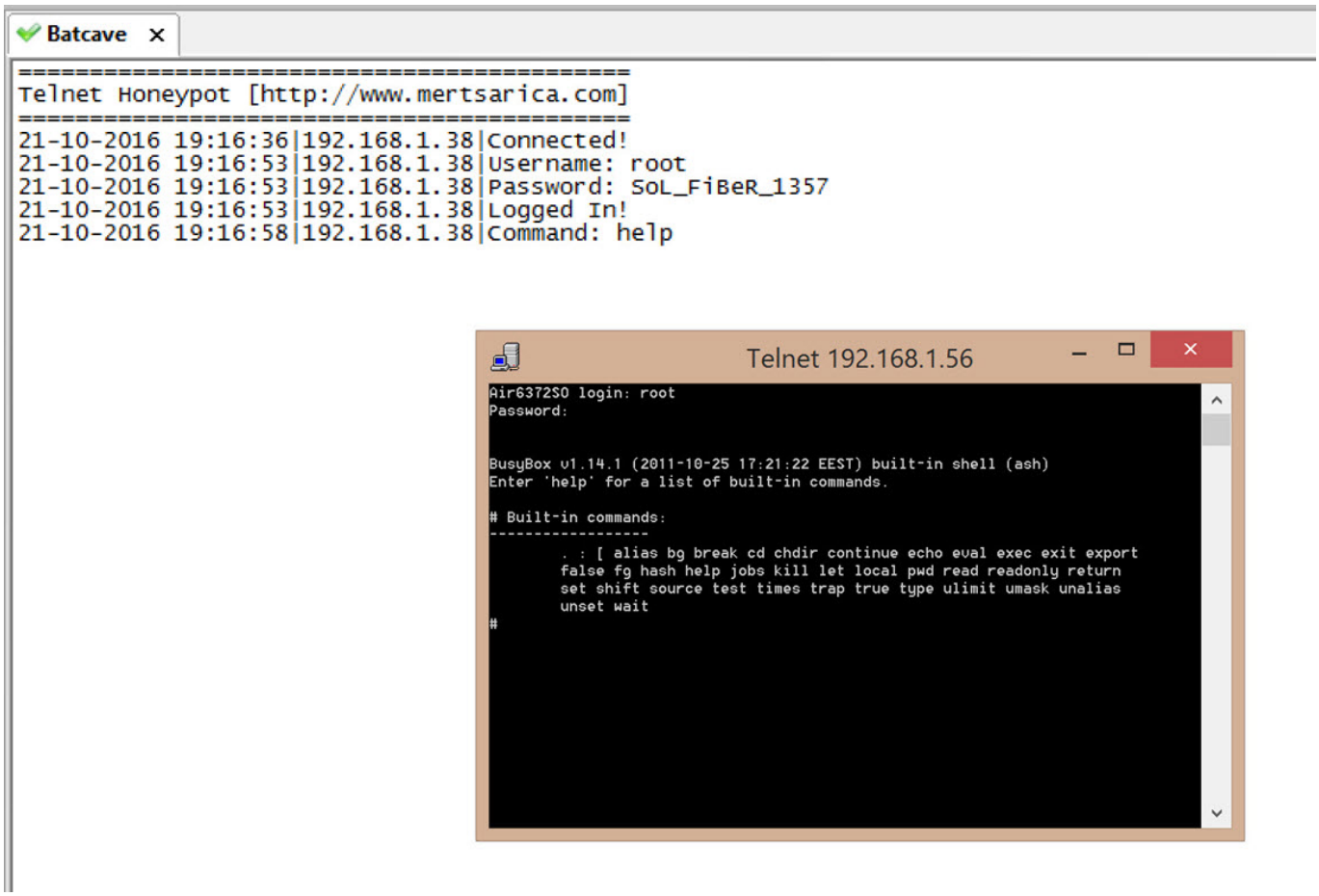
Mert bey merhaba, 2 gün önce başımız geldi, 2 ay öncede İstanbuldaki bir firmaya. Müşteride tüm veritabanlarını ve ortak kulannılan dosyaları şifrediler ve para istiyorlar. Bu konuda 3389 portu haricinde yapılabilecekler, alınması gereken önlemler konusunda yardımcı olabilirmisiniz. Vatandaşlar Active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

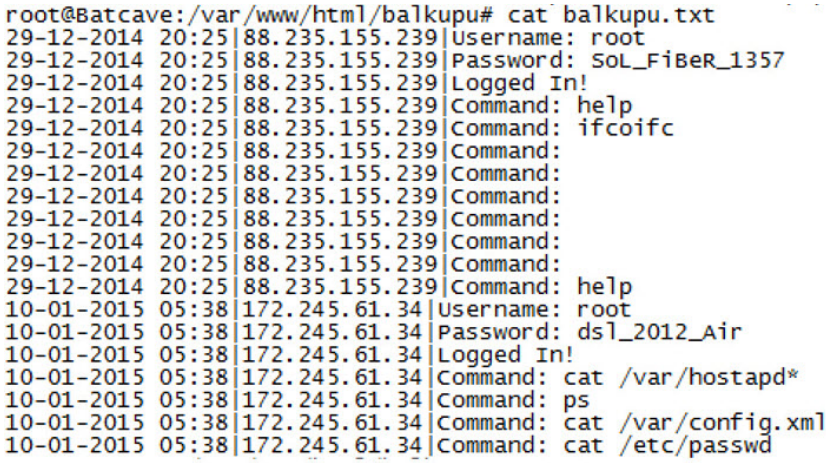
In my blog post "Virtual Siege" that I wrote in 2010, I set up a simple honeypot at my home, and the point I was trying to make with the following sentence was that the problems faced by end users today in the virtual world were almost like echoes of what I had highlighted in the post.

"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 “Air6372SO 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.





Towards the end of 2016, I decided to shed light on the methods used by ransomeware 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**

★★★★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

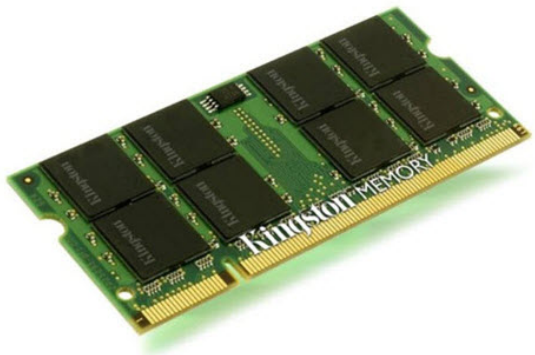
Favori Listeme Ekle | Karşılaştır | Fiyat Alarmı

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	

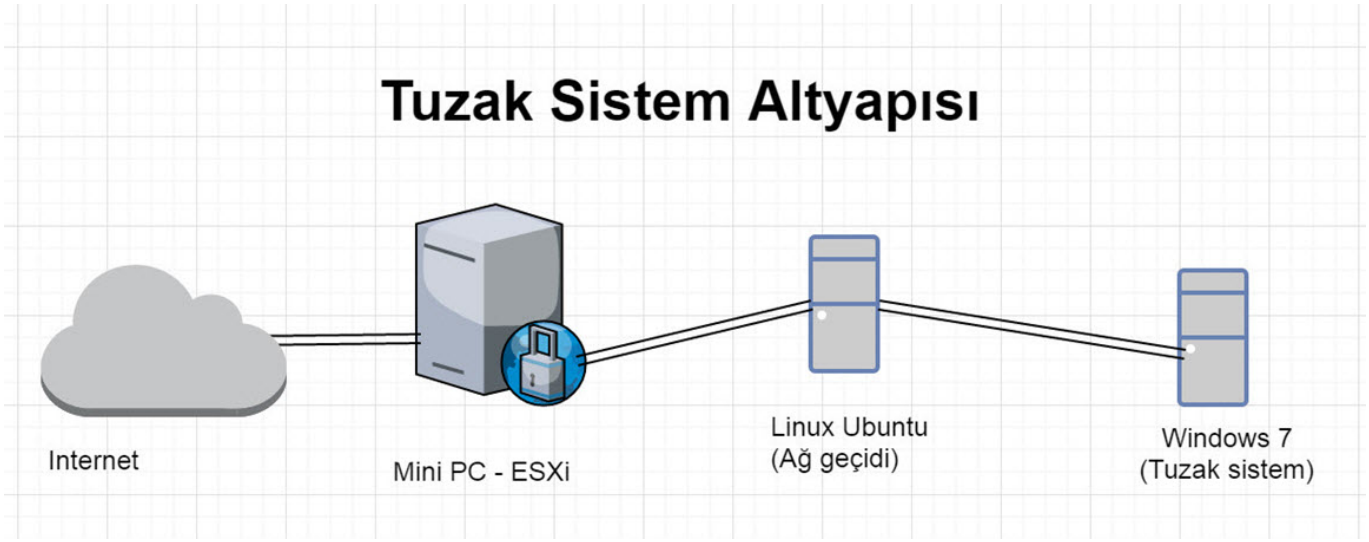
Recent Tasks

Name, Target or Status contains: Clear

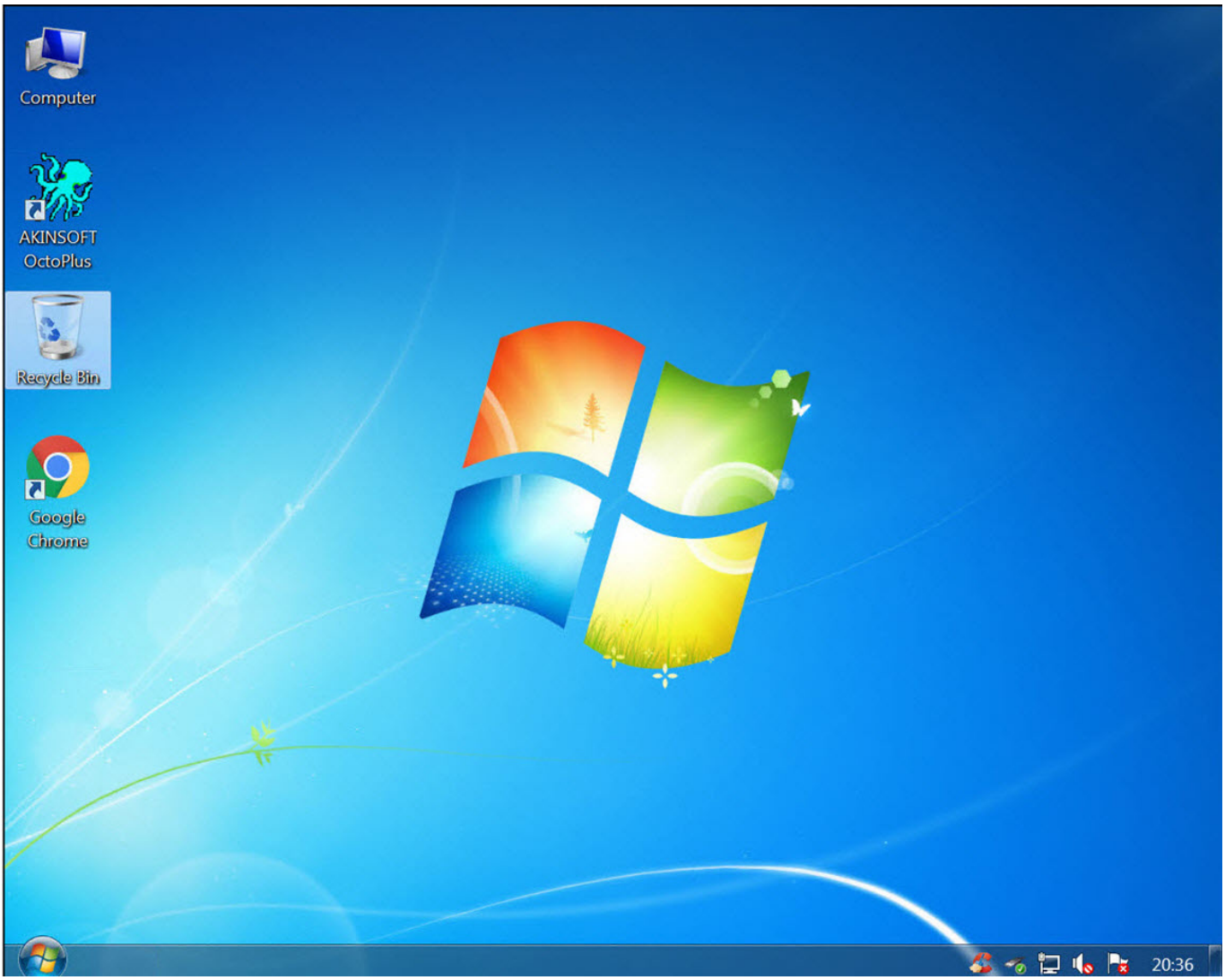
Name	Target	Status	Details	Initiated by	Requested Start Ti...	Start Time	Completed Time

Tasks

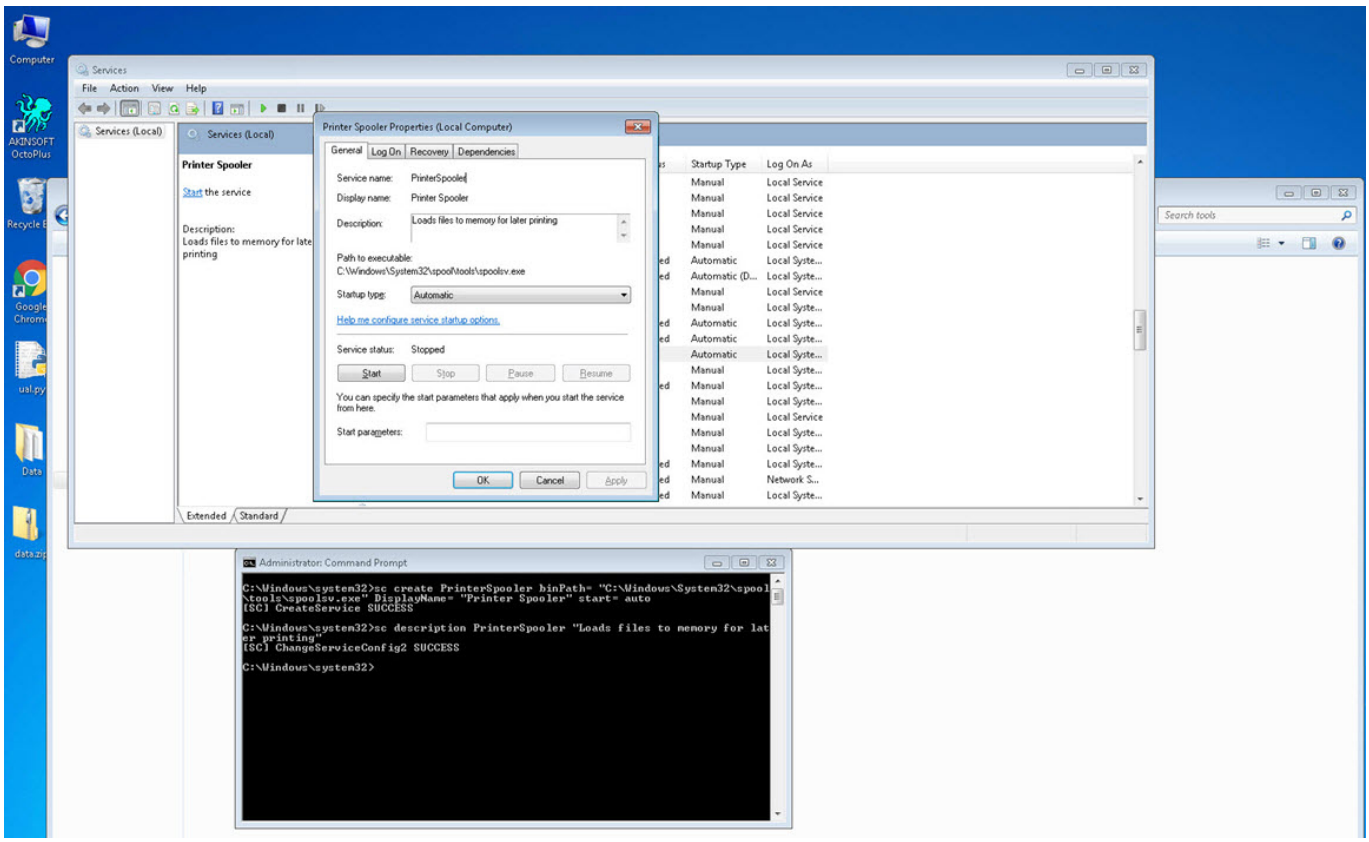
To release cursor, press CTRL+ALT root



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 Akınsoft's OctoPlus software.

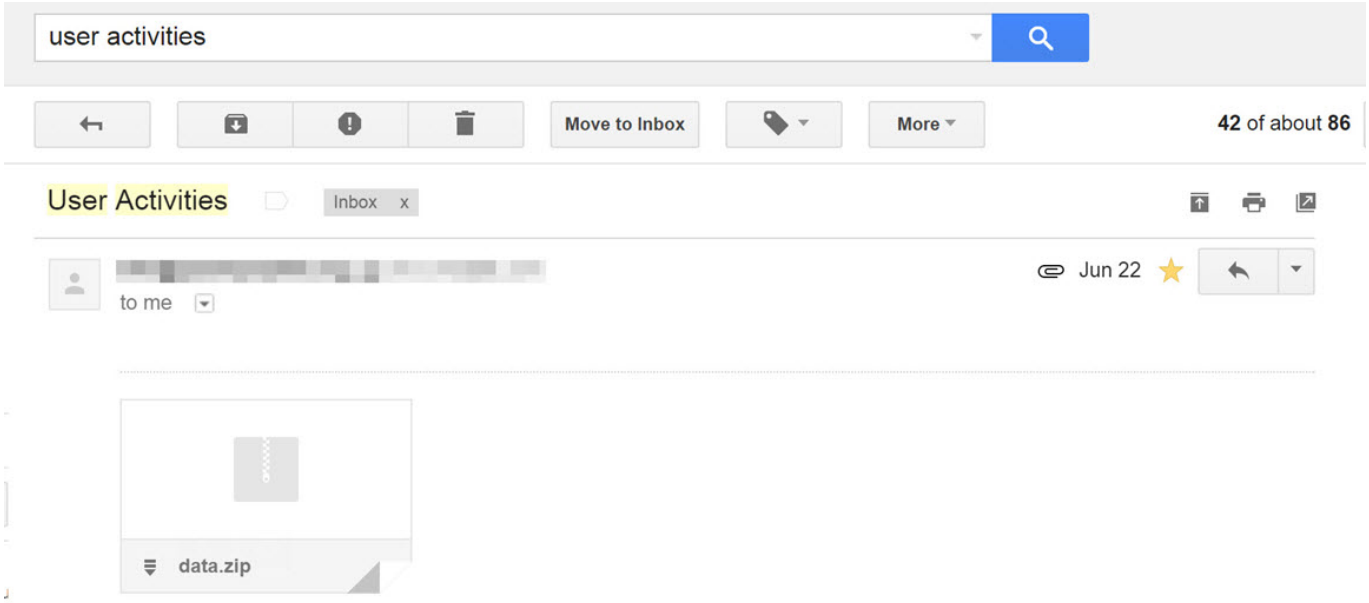


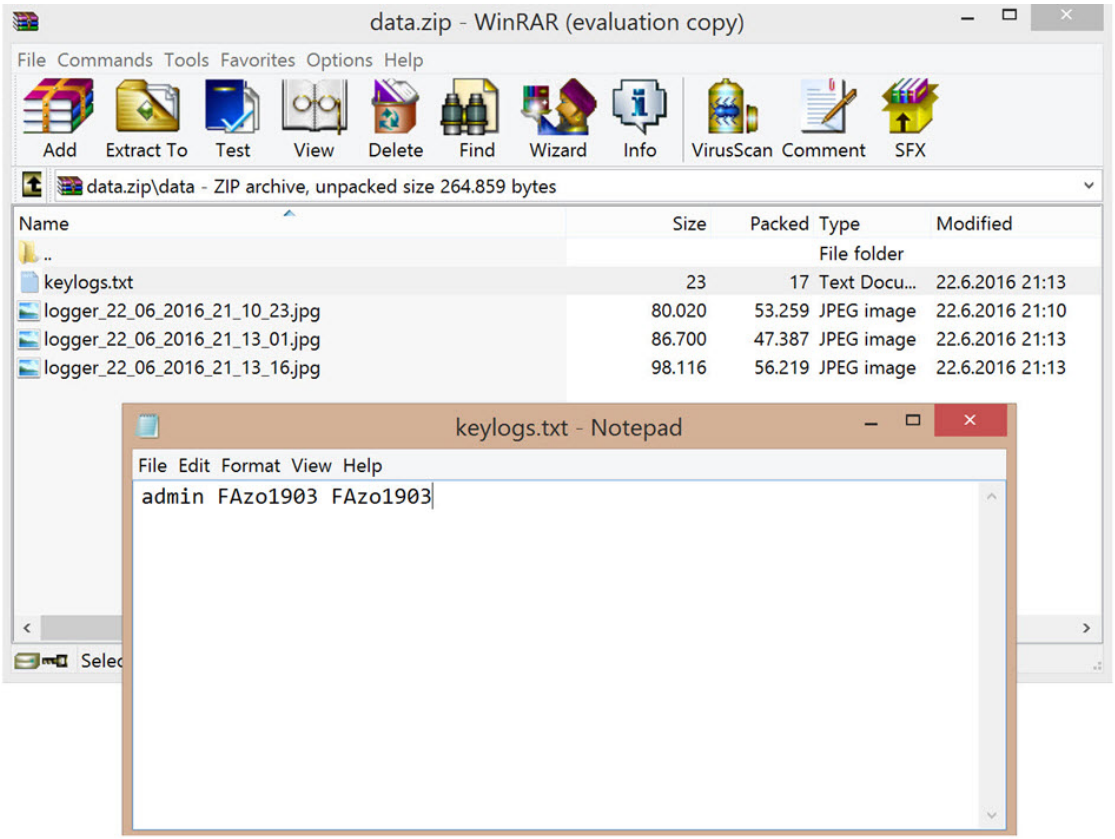
When it came time to design the tool that would make the deception system a trap, I created a tool called UAL (User Activity Logger) using Python. It would record all of the user's actions on Windows (keystroke logging, video recording, screen capture, clipboard copying) and sends all information except 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 ransomeware attackers, who targeted individuals and made the news, encrypting data and leaving a note, to fall

into the deception system.




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

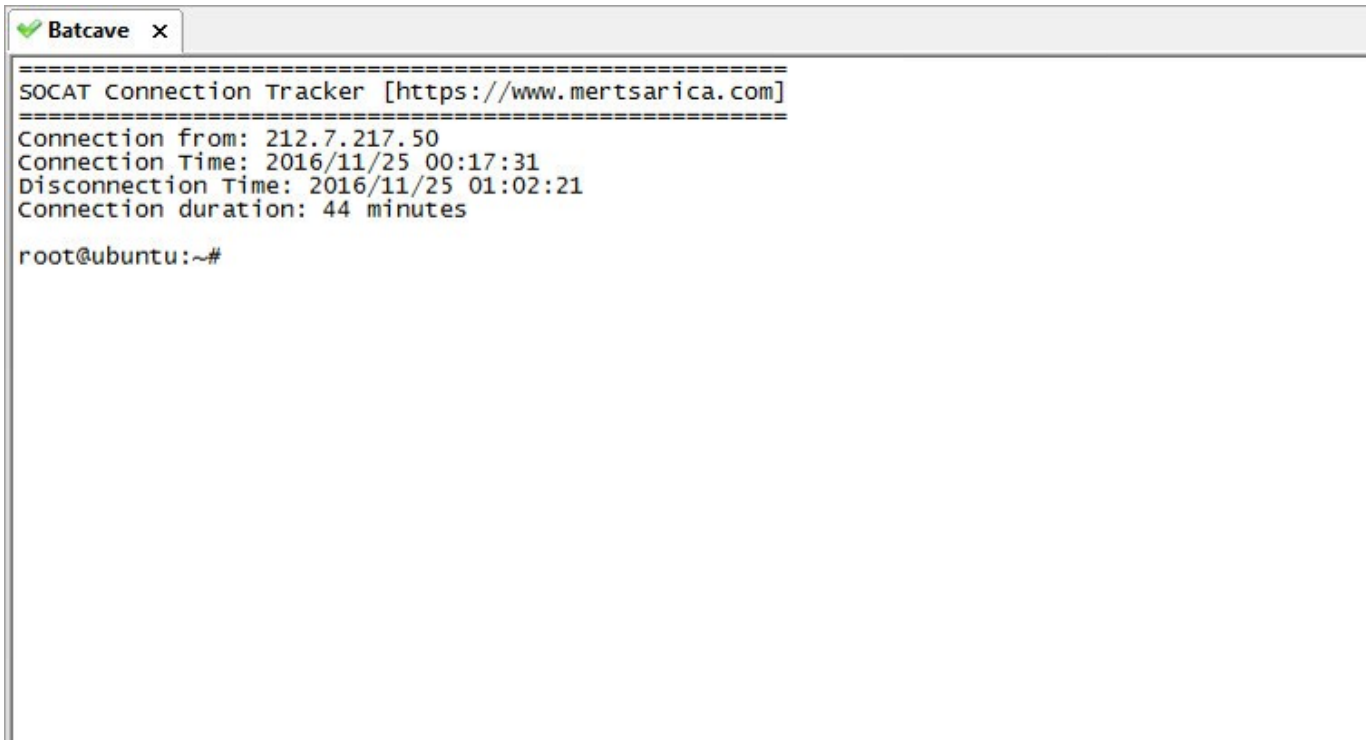
Polis 2011 yılından beri yaptığı araştırmada, incelenen 273 olayın 271'inde bir ize ulaşılamadığı ancak 2 olayda yapılan hata sayesinde şebeke ele başı S.B.'ye ulaşıldı. Ukrayna'da yaşayan Türk vatandaşı bilgisayar mühendisi S.B.'nin 3 ay önce Türkiye'ye giriş yaptığı belirlendi. Polis S.B.'nin irtibatlarını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

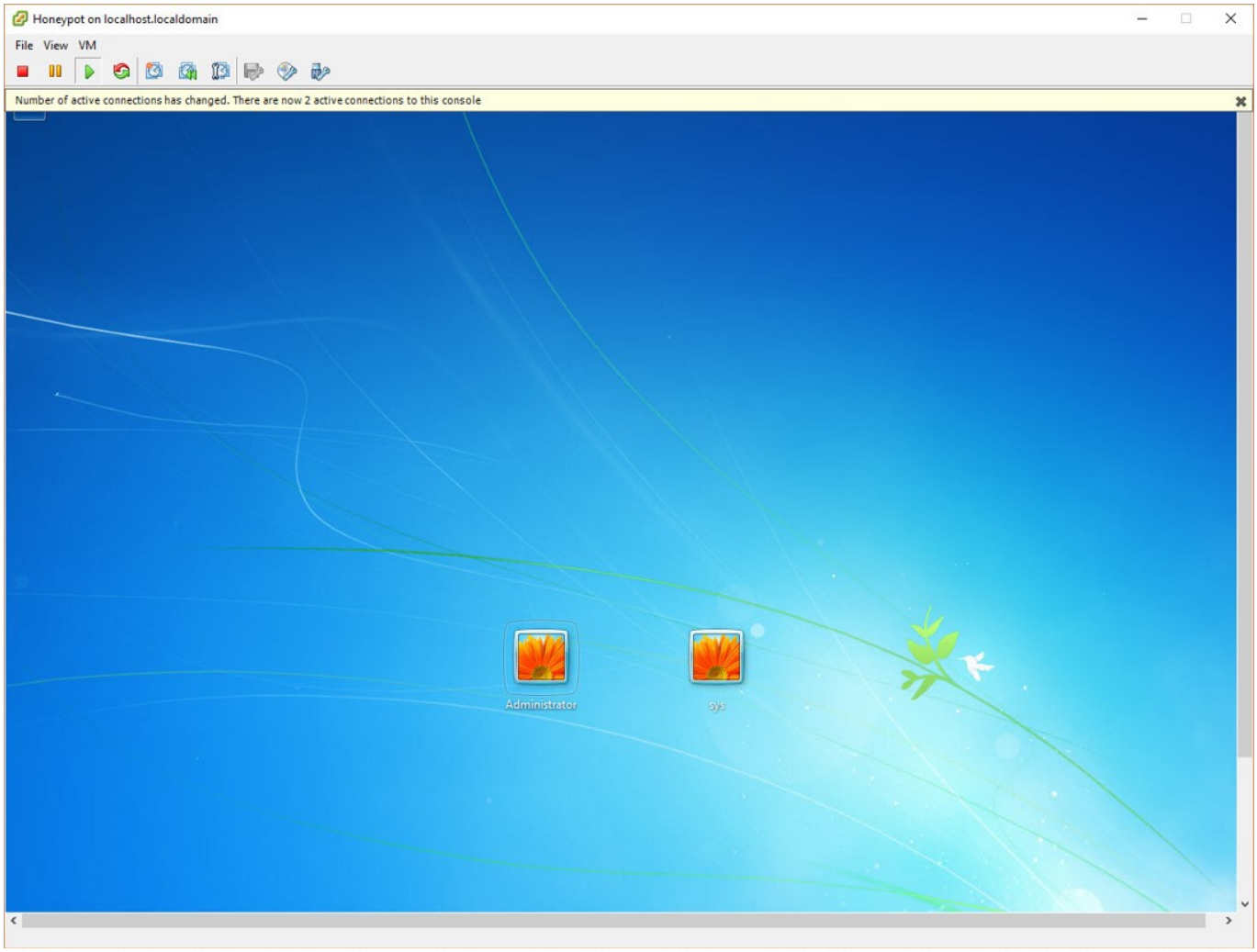
Polis şebekenin para aldığı şirketlerle ilgili çalışmalarına devam ederken, şebekenin, şu ana kadar yapılan tespitlerde 55 şirketten 87 bin 684 Dolar alındığı belirlendi. Paraların şebekenin talebi üzerine Rusya, Ukrayna, Çin Vietnam, Peru gibi ülkelerdeki hesaplara havale edildiği belirlendi. Bu ülkelere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

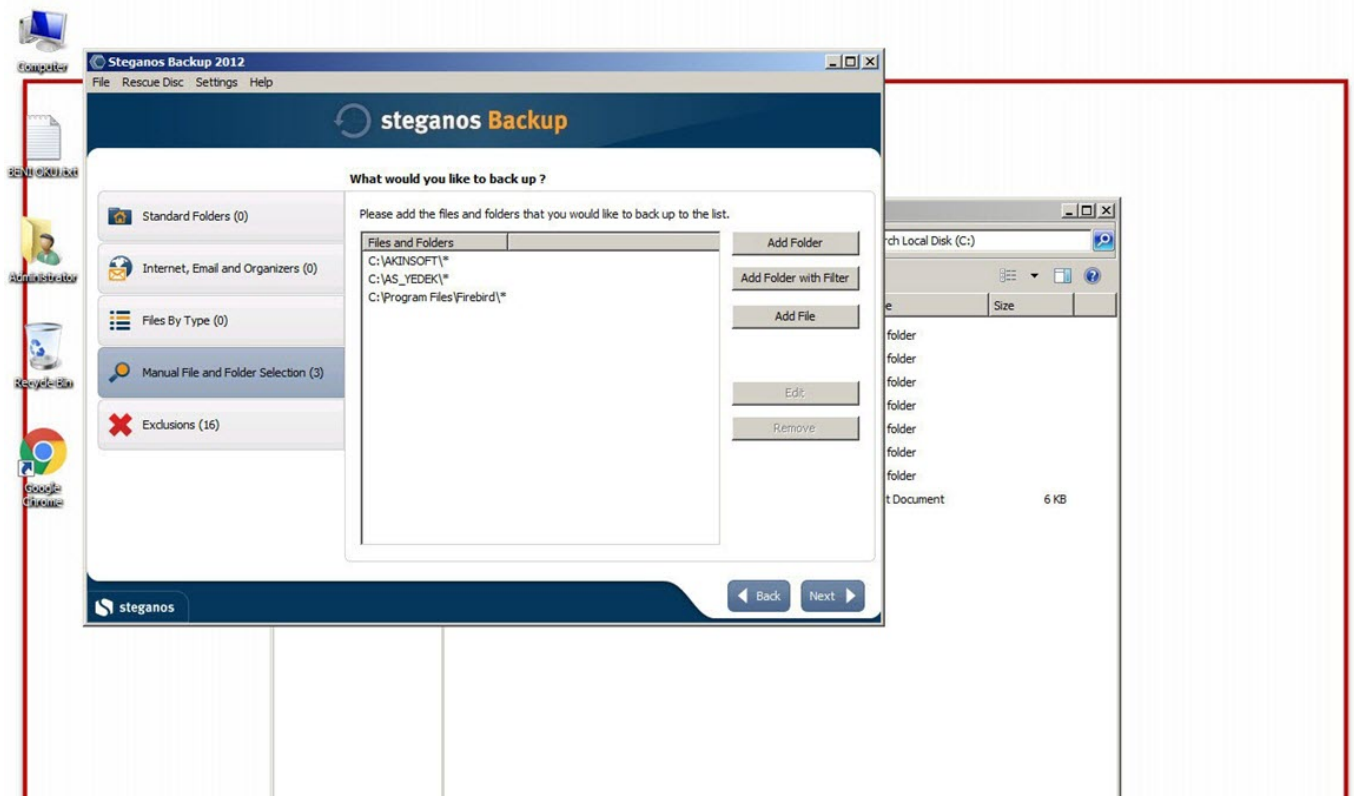
To be able to know the IP addresses of those who connect to the trap system and how long they stayed connected, I decided to redirect connections through Ubuntu (Batcave) instead of allowing internet access to the Remote Desktop service. To do this, I used the socat tool on Ubuntu to redirect all requests 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

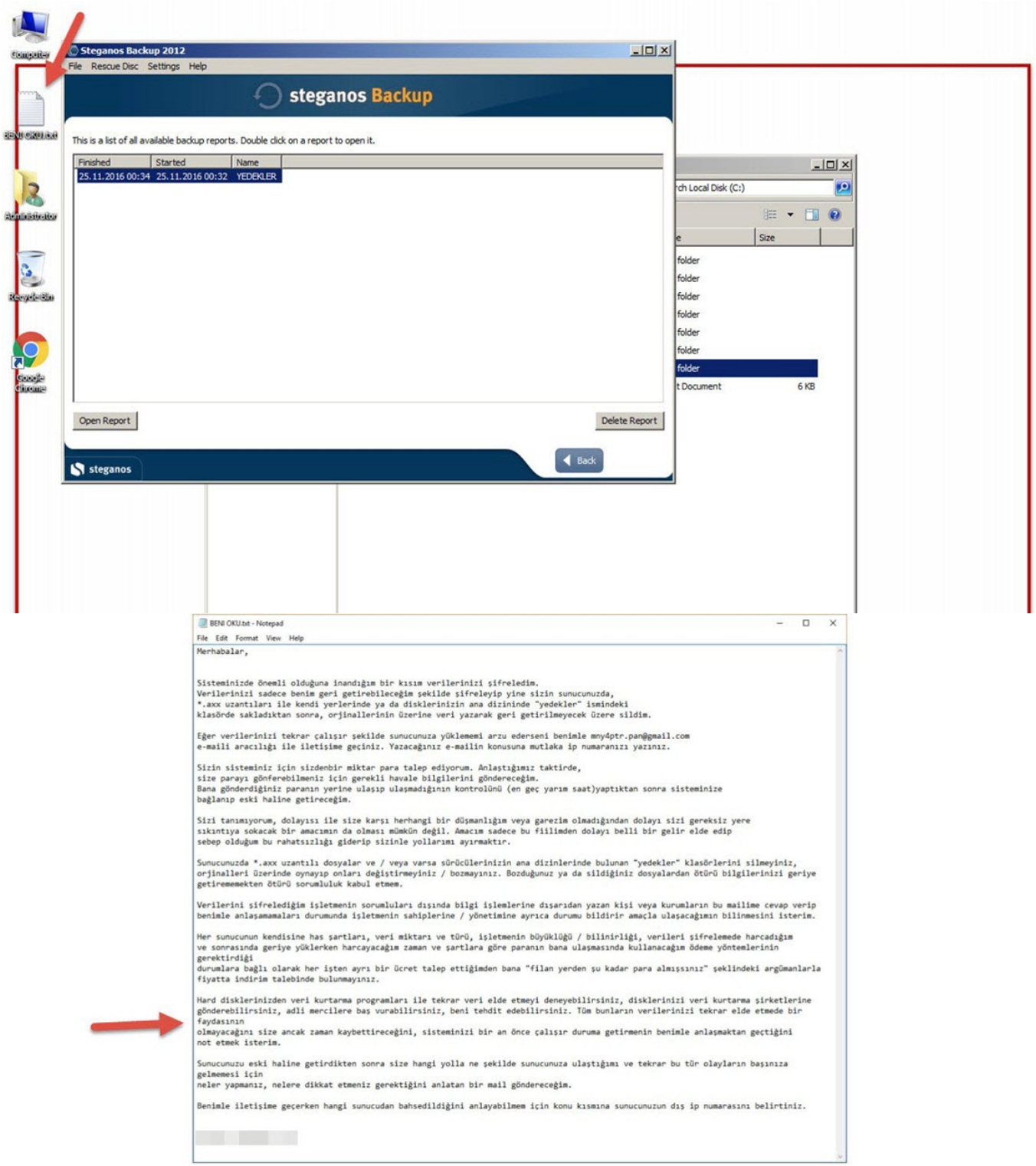
in Python called Socat Connection Tracker to help in monitoring connections.



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.

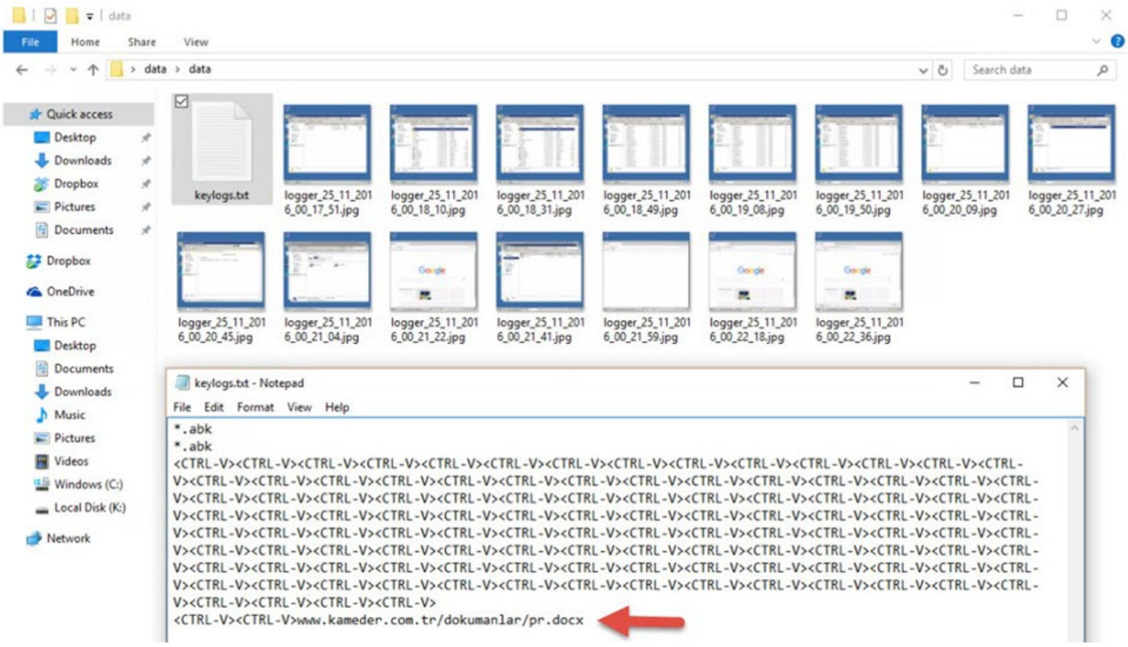

Honeypot on localhost.localdomain
File View VM
Number of active connections has changed. There are now 2 active connections to this console
Administrator
sys

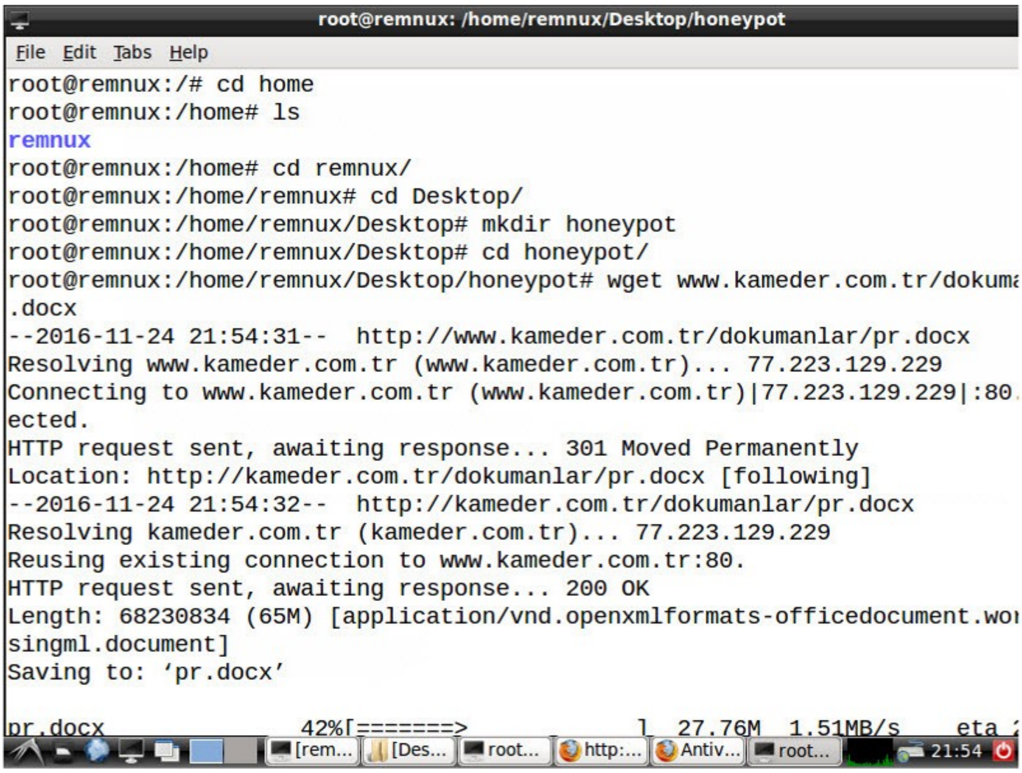

Steganos Backup 2012
File Rescue Disc Settings Help
steganos Backup
What would you like to back up ?
Standard Folders (0)
Internet, Email and Organizers (0)
Files By Type (0)
Manual File and Folder Selection (3)
Exclusions (16)
Please add the files and folders that you would like to back up to the list.
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

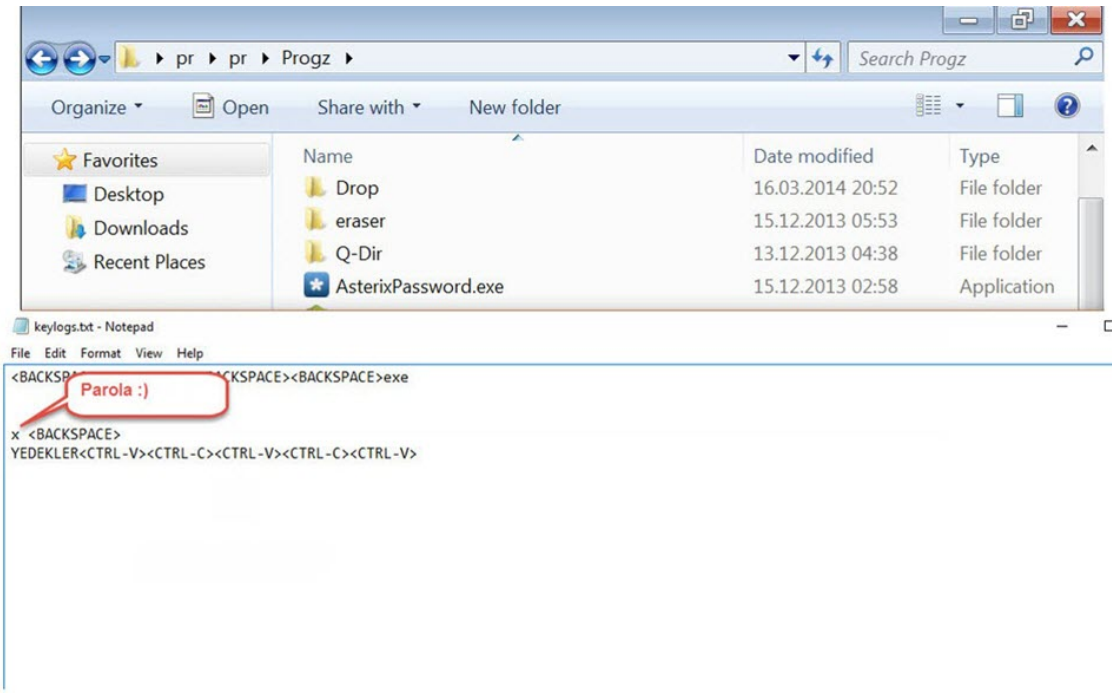


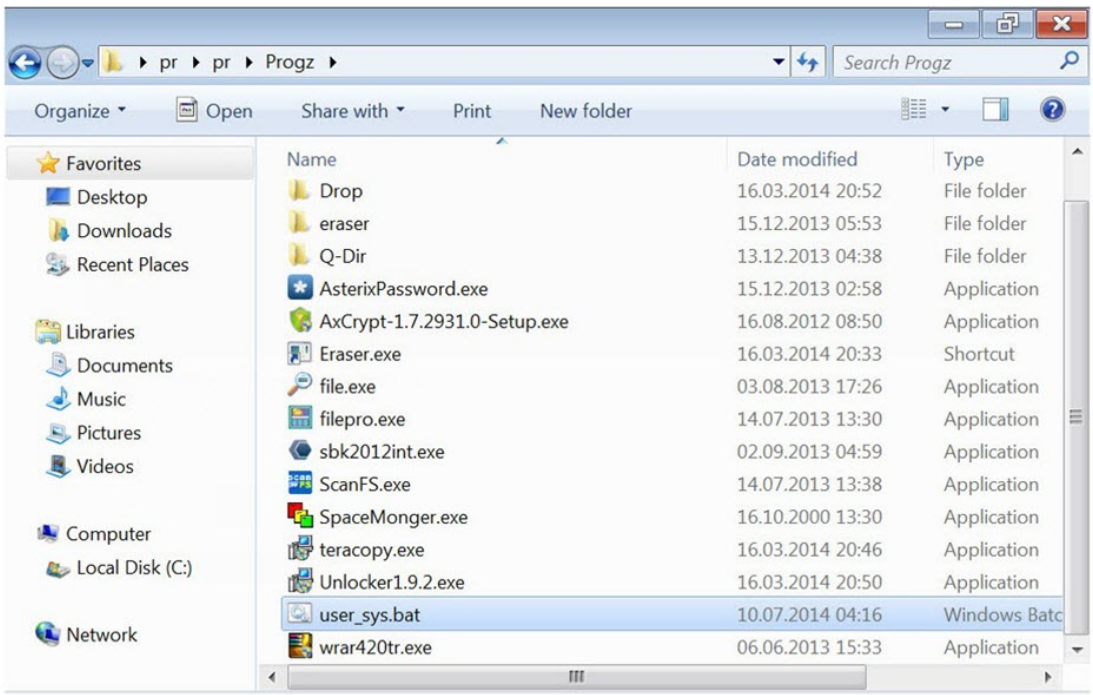
Upon reviewing the records of the malicious person, I found that he had downloaded a file named “pr.docx” from a website (likely a hacked one) called kameder.com.tr. Because the file was a 65 MB document, it seemed suspicious and I was able to find out that it was a ZIP file. When I tried to open the 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

finding the password for the “Sys” user in a bat file, I continued to search for similar files in case it contained the password for my encrypted files, but found no such file.






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>

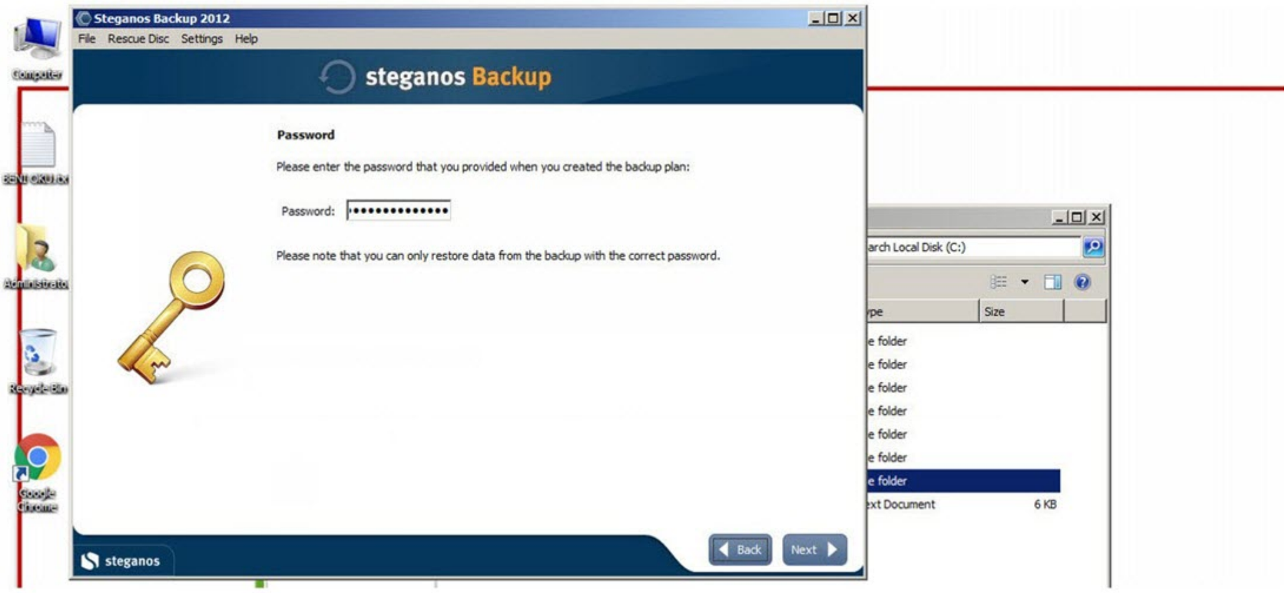

pr ▸ pr ▸ Progz ▸
Search Progz
Organize
Open
Share with
Print
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
Network
Name
Date modified
Type
Drop
16.03.2014 20:52
File folder
eraser
15.12.2013 05:53
File folder
Q-Dir
13.12.2013 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

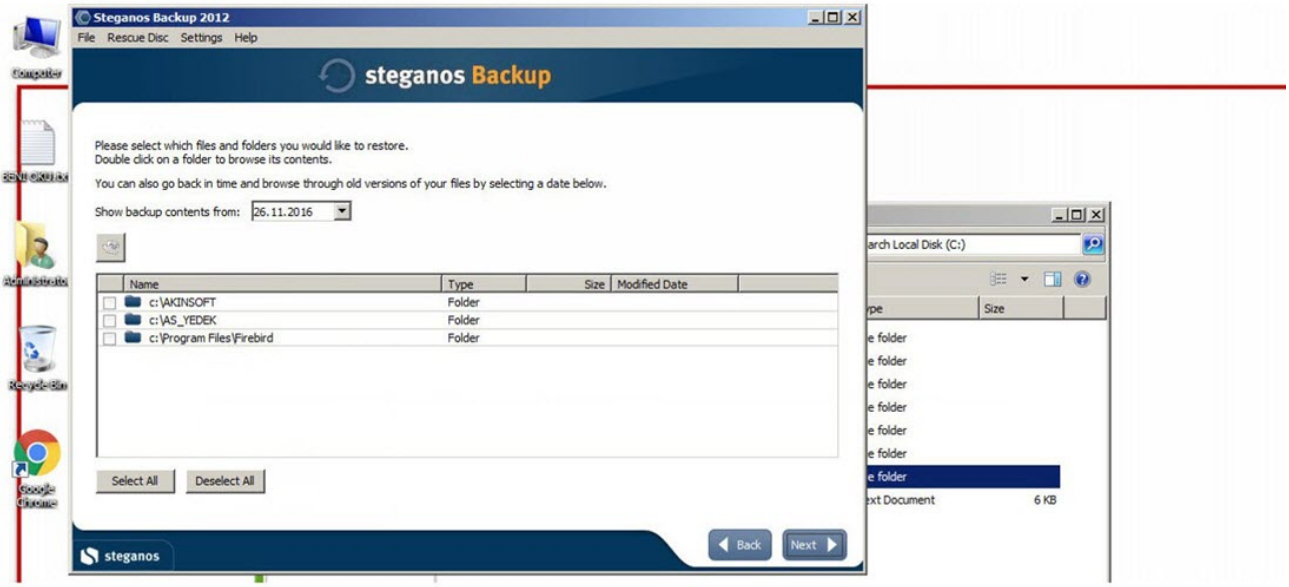
user_sys.bat

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

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.

keylogs.txt - Notepad
File Edit Format View Help
v<CTRL-
V>SEMSIPASAPASASINDASESIBUZUSESICELER<BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE
><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><B
ACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACK
SPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPA
CE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE>
<BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BA
CKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE>SEMSIPASAPASASINDA
<BACKSPACE><BACKSPACE>SES<BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE>
<BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BA
CKSPACE><BACKSPACE><BACKSPACE><BACKSPACE>SEMSIP<BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE>
<BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BA
CKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKS
PACE><BACKSPACE><BACKSPACE>SEMSIPASAPASASINDASESIBUZUSESICELER<TAB>SEMSIPASAPASASINDASESIBUZUSESICELER▯karsiyaka2322040<TAB>karsiyaka323
▯dvdas<BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPA
E><BACKSPACE><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.
Back
Next
steganos
Local Disk (C:)
Size
ext Document
6 KB



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.