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.

✓ Batcave ×

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!

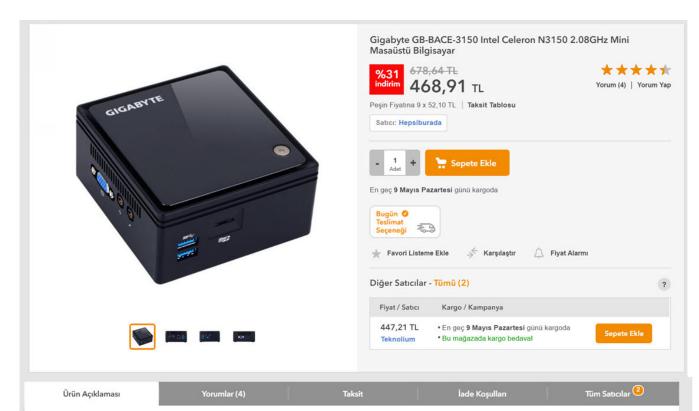
21-10-2016 19:16:55 192.168.1.38 Command: help



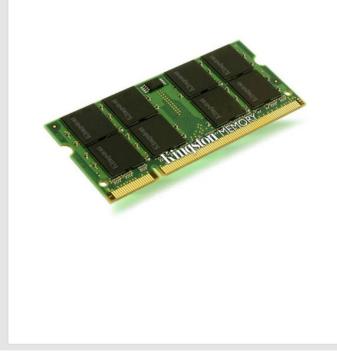
root@Batcave:/var/www/html/balkupu# cat balkupu.txt	
29-12-2014 20:25 88.235.155.239 Username: root	
29-12-2014 20:25 88.235.155.239 Password: SoL_FiBeR_1357	
29-12-2014 20:25 88.235.155.239 Logged In!	
29-12-2014 20:25 88.235.155.239 Logged In! 29-12-2014 20:25 88.235.155.239 Command: help	
29-12-2014 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: 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 05-20 172 245 61 24 Semmends as	
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 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).

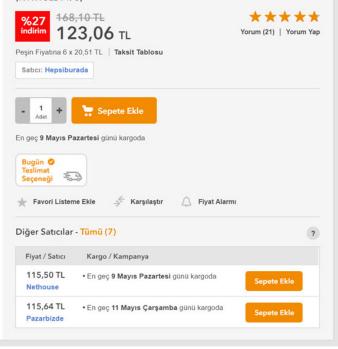
After collecting the hardware, I ended up with a deception system that had a 2GHz processor, 8GB of RAM, and a 120GB SSD disk. So first, I installed the free ESXi virtualization system, and on top of that, I installed a Windows 7 (Honeypot) with a fake accounting application to catch malicious individuals 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.

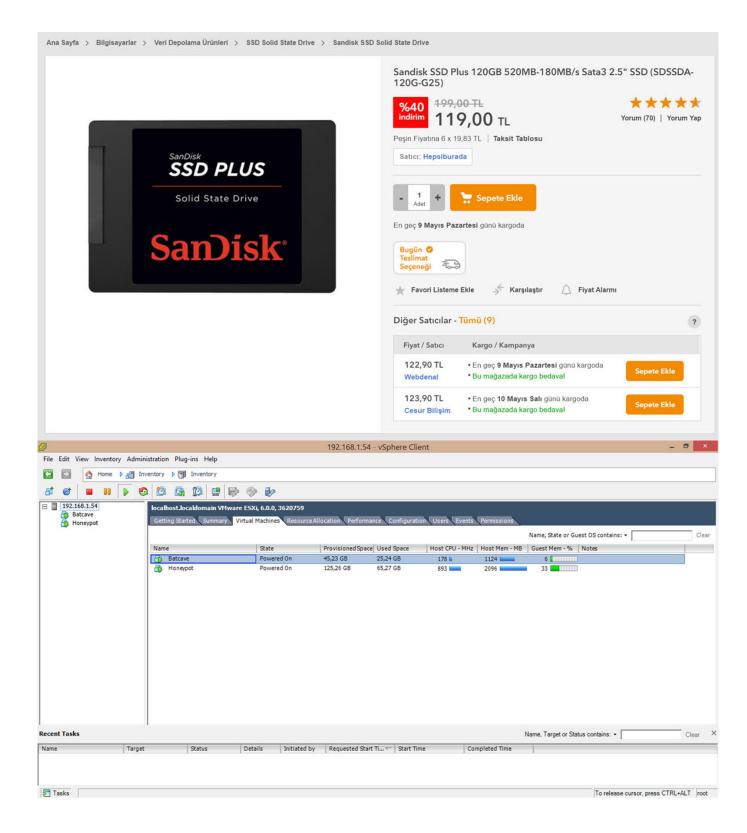


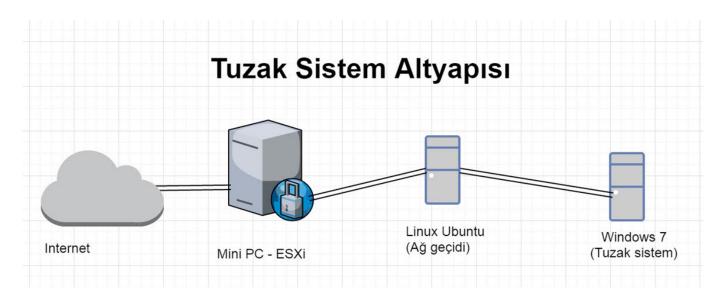
Marka	Gigabyte	
şlemci Tipi	Intel Celeron	
şlemci Hızı	2 GHz	
şlemci Cache	2 MB cache	
Ram Tipi	DDR3	
Ekran Kartı Tipi	Dahili Ekran Kartı	
Ekran Kartı Modeli	Paylaşımlı	
Monitör	Yok	
3D Desteği	Yok	
Wireless Özelliği	802.11 n	
Kimin Seçimi	Günlük	



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



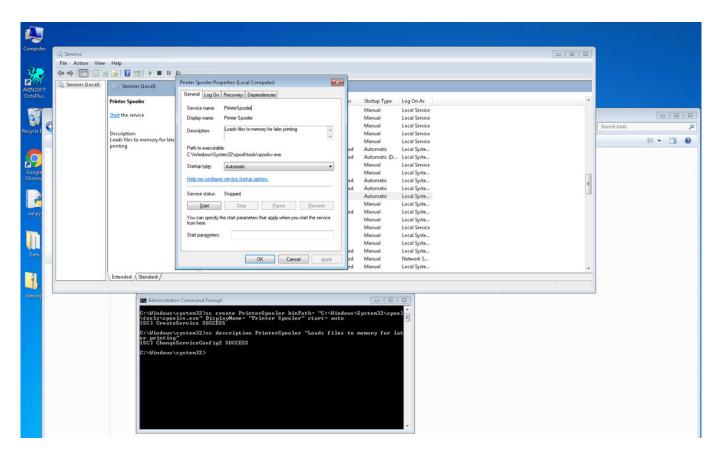




To make the deception system more attractive to malicious individuals, I began searching for an accounting software to install on the Windows 7-based system. To decide which accounting software to use, I used information I had gathered from victims of data encryption and chose Akinsoft's OctoPlus software.



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 ransomeware attackers, who targeted individuals and made the news, encrypting data and leaving a note, to fall

into the deception system.

user ac	ivities 🗸	Q
+	Move to Inbox More - More -	42 of about 8
<mark>User</mark> A	ctivities D Inbox x	
to	me 💌	🗢 Jun 22 ★ 🔺 🔻
	╤ data.zip	
	⊊ uata.zip	
<pre></pre>	data 6 items	
	🖹 keylogs.txt	
≢ da	Logger_22_06_2016_21_19_35.jpg	
	Logger_22_06_2016_21_19_51.jpg	
o@za	Logger_22_06_2016_21_20_06.jpg	
me i	logger_22_06_2016_21_20_37.jpg	
	Iogger_22_06_2016_21_20_53.jpg	
= da		

ile Comma	ands Tools Favori				aluation cop	,,	
17	ktract To Test	00	Delete Find	Wizard	Info Viru	sScan Comment SI	-x
🚹 🗃 data	a.zip\data - ZIP arc	hive, unpack	ed size 264.85	9 bytes			
lame		^			Size	Packed Type	Modified
.						File folder	
keylogs.t	xt				23	17 Text Docu.	22.6.2016 21:13
	2_06_2016_21_10_				80.020	53.259 JPEG image	
	2_06_2016_21_13_ 2_06_2016_21_13_				86.700 98.116	47.387 JPEG image 56.219 JPEG image	
			keyl	ogs.txt - N	lotepad	_ [×
	File Edit Forma	t View Hel		9			
	admin FAzo	1903 FAzo	01903				×.
J⊶⊡ Selec	¢						

Bilgisayar korsanlarına operasyon

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

Yorum yaz

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.



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

DHA

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.

() Harrison	t en la sella est la sel da serie				
File View	t on localhost.localdomain /M				- • ×
• •• [the second secon	÷			
Number of ac	tive connections has changed. There are now 2	active connections to this console			×
9					
				A A A	
		Administrator	sys		
۲					>
	C Steganos Backup 2012		×	1	
	File Rescue Disc Settings Help			-	
		🔵 steganos Backup			
		0			
RENIL CRUDER		What would you like to back up?			
	Standard Folders (0)	Please add the files and folders that you would like to back up to the		X	
12	A Internet Empland Graphings (0)	Files and Folders C:\AKINSOFT*	Add Folder	rch Local Disk (C:)	
<u>Arminiki der</u>	Internet, Email and Organizers (0)	C:\AS_YEDEK\" C:\Program Files\Firebird\"	Add Folder with Filter		
-	Files By Type (0)		Add File	e Size folder	
Service Bin				folder	
Recyclettio	Manual File and Folder Selection (3)		Edit	folder	
	Exclusions (16)		Remove	folder folder	
$\left \right\rangle$				folder	
cionejte: Citiconte:				folder t Document 6 KB	
and the					

🖣 Back Next 🕨

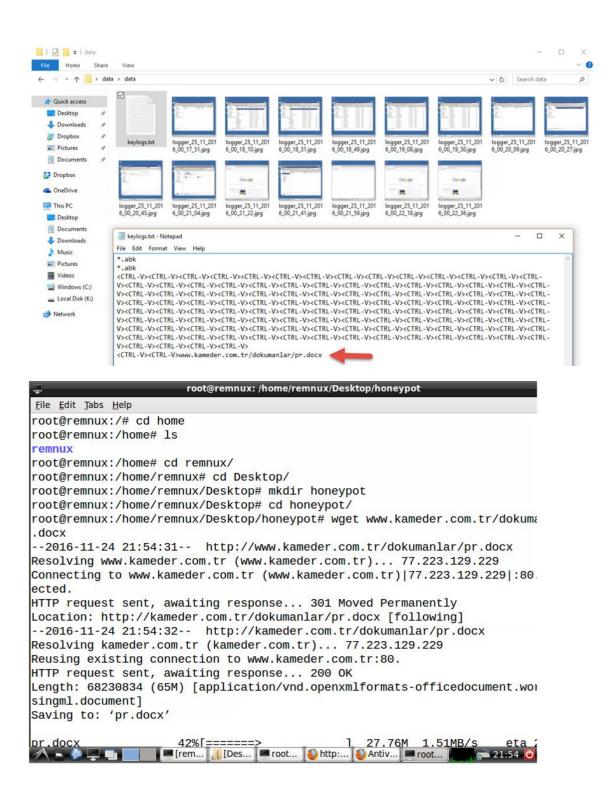
6 KB

S steganos

Coogle Classice

	/	
Compaties	Steganos Backup 2012	
	File Rescue Disc Settings I	
		Steganos Backup
REAL CONTROL	This is a list of all available bac	up reports. Double click on a report to open it.
	Finished Started	Name - D X
12	25.11.2016 00:34 25.11.20	16 00:32 YEDBALER The Local Disk (C:)
Anniekikality		
		e Size
3		folder
Recycle Bio		folder folder
		folder
		folder folder
Coosile		folder
Chrome		t Document 6 KB
	Open Report	Delete Report
		■ Back
	S steganos	Dock
		I BEN CRUstri - Notepad - □ X File Edit Format View Help
		Merhabalar,
		Sisteminizde önemli olduğuna inandığım bir kısım verilerinizi şifreledim. Verilerinizi sadece benim geri getirebileceğim şekilde şifreleyip yine sizin sunucunuzda,
		*.axx uzantıları ile kendi yerlerinde ya da disklerinizin ana dizininde "yedekler" ismindeki klasörde sakladıktan sonra, orjinallerinin üzerine veri yazarak geri getirilmeyecek üzere sildim.
		Eger verilerinizi tekrar çalışır şekilde sunucunuza yüklememi arzu ederseni benimle mny4ptr.pan@gmail.com e-maili aracılığı ile iletişime geçiniz. Yazacağınız e-mailin konusuna mutlaka ip numaranızı yazınız.
		Sizin sisteminiz için sizdenbir miktar para talep ediyorum. Anlaştığımız taktirde,
		size parayı gönferebilmeniz için gerekli havale bilgilerini göndereceğim. Bana gönderdiğiniz paranın yerine ulasıp ulaşmadığının kontrolünü (en geç yarım saat)yaptıktan sonra sisteminize bağlanı eski halime gerineceğim.
		Sizi tanımıyorum, dolayısı ile size karşı herhangi bir düşmanlığım veya garezim olmadığından dolayı sizi gereksiz yere
		sıkıntıya sokacak bir amacımın da olması mümkün değil. Amacım sadece bu fiilimden dolayı belli bir gelir elde edip sebep olduğum bu rahatsızlığı giderip sizinle yollarımı ayırmaktır.
		Suncunuzda *.axx uzantil dosyalar ve / veya varsa sürücülerinizin ana dizinlerinde bulunan "yedekler" klasärlerini silmeyiniz, orjinalleri üzerinde oynayız onları değistirmeyiniz / bozmayınız. Bozduğumuz ya da sildiğiniz dosyalardan ötürü bilgilerinizi geriye getirmemsetken ötürü sorvaluluk kabul etmem.
		Verilerini şifrelediğim işletmenin sorumluları dışında bilgi işlemlerine dışarıdan yazan kişi veya kurumların bu mailime cevap verip benimle anlaşamamaları durumunda işletmenin sahiplerine / yönetimine ayrıca durumu bildirir amacla ulaşacağımın bilinmesini isterim.
		Her sunucunun kendisine has şartları, veri miktarı ve türü, işletmenin büyüklüğü / bilinirliği, verileri şifrelemede harcadığım ve sonrasında geriye yüklerken harcayacağım zaman ve şartlara göre paranın bana ulaşmasında kullanacağım ödeme yöntemlerinin serektirdiği
		gerektirolgi durumlara bağlı olarak her işten ayrı bir ücret talep ettiğimden bana "filan yerden su kadar para almışsınız" şeklindeki argümanlarla fiyatta indirim talebinde bulunmayınız.
		Hard disklerinizden veri kurtarma programları ile tekrar veri elde etmeyi deneyebilirsiniz, disklerinizi veri kurtarma şirketlerine gönderebilirsiniz, adli mercilere baş vurabilirsiniz, beni tehdit edebilirsiniz. Tüm bunların verilerinizi tekrar elde etmede bir
	-	faydasının olmayacağını size ancak zaman kaybettireceğini, sisteminizi bir an önce çalışır duruma getirmenin benimle anlaşmaktan geçtiğini not etmek isterim.
		Sunucunuzu eski haline getirdikten sonra size hangi yolla ne şekilde sunucunuza ulaştığımı ve tekrar bu tür olayların başınıza gelmemesi icin
		neler yapmanız, nelere dikkat etmeniz gerektiğini anlatan bir mail göndereceğim.
		Benimle iletişime geçerken hangi sunucudan bahsedildiğini anlayabilmem için konu kısmına sunucunurun dış ip numarasını belirtinir.

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.

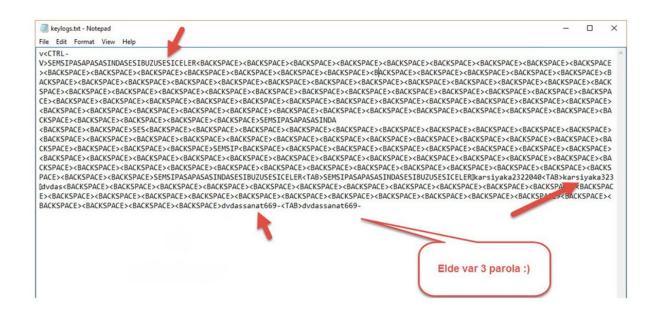


Organize • 🖻 Op			
🚖 Favorites	Name	Date modified	Туре
💹 Desktop	📙 Drop	16.03.2014 20:52	File folder
bownloads	📙 eraser	15.12.2013 05:53	File folder
Skecent Places	📙 Q-Dir	13.12.2013 04:38	File folder
	🚼 AsterixPassword.exe	15.12.2013 02:58	Application
Parola :)	PACE> <backspace>exe</backspace>		
le Edit Format View Help			
le Edit Format View Help BACKSP Parola :) <backspace></backspace>			
le Edit Format View Help BACKSP Parola :) <backspace></backspace>			
le Edit Format View Help BACKSP Parola :) <backspace></backspace>			

Organize 🔹 📄 Ope	n Share with 👻 Print New folder		II • 🗍 🔞
	Name	Date modified	Туре
E Desktop	📕 Drop	16.03.2014 20:52	File folder
Downloads	🐌 eraser	15.12.2013 05:53	File folder
Recent Places	📕 Q-Dir	13.12.2013 04:38	File folder
J Heteric Hates	\star AsterixPassword.exe	15.12.2013 02:58	Application
Libraries	😪 AxCrypt-1.7.2931.0-Setup.exe	16.08.2012 08:50	Application
Documents	Eraser.exe	16.03.2014 20:33	Shortcut
Jocuments Music	🔎 file.exe	03.08.2013 17:26	Application
Pictures	🔚 filepro.exe	14.07.2013 13:30	Application
-	sbk2012int.exe	02.09.2013 04:59	Application
JUIDE VIDE VIDE VIDE VIDE VIDE VIDE VIDE V	3 ScanFS.exe	14.07.2013 13:38	Application
	CaraceMonger.exe	16.10.2000 13:30	Application
Computer	🞼 teracopy.exe	16.03.2014 20:46	Application
bocal Disk (C:)	🐻 Unlocker1.9.2.exe	16.03.2014 20:50	Application
	🕲 user_sys.bat	10.07.2014 04:16	Windows Bate
💐 Network	wrar420tr.exe	06.06.2013 15:33	Application

🔚 user_	_sys.bat 🔀
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.



	O atoma Dealan	
	🔿 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.	arch Local Disk (C:)
\bigcirc		8= • 🗊 😧
		pe Size
		e folder
~~		e folder
		e folder
		e folder e folder
		e folder
		e folder
		ext Document 6 KB
		UNU UNU
S steganos	A Back Ne	ext 🕨

lick on a folder to browse its contents. also go back in time and browse through old versions of your files by selecting a date below. doup contents from: 26.11.2016 ▼ ame Type Size Modified Date I c:VAS_YEDEK Folder 1 c:VAS_YEDEK FOLDER 1 c:VAS_YEDEK FOLE	dick on a folder to browse its contents. also go back in time and browse through old versions of your files by selecting a date below. adoup contents from: below: dame c:\ACINSOFT Folder c:\ACINSOFT	le dick on a folder to browse its contents. can also go back in time and browse through old versions of your files by selecting a date below. r backup contents from: 26.11.2016 ▼ b ct/AKINSOFT Folder F	u can also go back in time and browse its contents. Image: City Contents from: 25, 11, 2016 Image: City Contents fr	Name Type Size Modified Date arch Local Disk (C:) C : VACINSOFT Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder	le dick on a folder to browse its contents. an also go back in time and browse through old versions of your files by selecting a date below. Ibackup contents from: 25.11.2016 Ibackup contents from: 25.11.20
lick on a folder to browse its contents. also go back in time and browse through old versions of your files by selecting a date below. doup contents from: 26.11.2016 ▼ ame Type Size Modified Date I c:VAS_YEDEK Folder 1 c:VAS_YEDEK FOLDER 1 c:VAS_YEDEK FOLE	dick on a folder to browse its contents. also go back in time and browse through old versions of your files by selecting a date below. adoup contents from: below: dame c:\ACINSOFT Folder c:\ACINSOFT	le dick on a folder to browse its contents. can also go back in time and browse through old versions of your files by selecting a date below. r backup contents from: 26.11.2016 ▼ b ct/AKINSOFT Folder F	uble click on a folder to browse its contents. u can also go back in time and browse through old versions of your files by selecting a date below. ow backup contents from: 26.11.2016 Name Type Size Modified Date c:VACINSOFT Folder c:VAS_YEDEK Folder c:VProgram Files/Firebird Folder folde	uble didk on a folder to browse its contents. u can also go back in time and browse through old versions of your files by selecting a date below. ow backup contents from: 26.11.2016 Name Type Size Modified Date C (VACINSOFT Folder Fol	le dick on a folder to browse its contents. an also go back in time and browse through old versions of your files by selecting a date below. Ibackup contents from: 25.11.2016 Ibackup contents from: 25.11.20
dup contents from: 26.11.2016 ame Type Size Modified Date arch Local Disk (C:) arch Local Disk (C:) arch Local Disk (C:) pe Size pe Size e folder e folder e folder e folder e folder	adup contents from: 26.11.2016 tame Type Size Modified Date if wCINSOFT Folder C:\WCINSOFT Folder C:\YS_YEDEX Folder f	v badup contents from: 26.11.2016 ▼ Name Type Size Modified Date C:\VASURSOFT Folder C:\VASURSOFT Folder C:\VASURSOFT Folder Folder C:\VasUrsoft Folder	w backup contents from: 26.11.2016 Image: Size Modified Date arch Local Disk (C:) Image: Size Civic Modified Date Image: Size Modified Date Image: Size Civic Modified Date Image: Size Modified Date Image: Size Civic Modified Date Image: Size Modified Date Image: Size Civic Modified Date Image: Size Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Imag	ow backup contents from: 26.11.2016 Image: Size Modified Date arch Local Disk (C:) Image: Size Club City City City City City City City City	Ibackup contents from: 26.11.2016 Name Type Size Modified Date Image: Ci VACINSOFT Folder Image: Ci VACINSOFT Folder Image: Ci VACINSOFT Folder Image: Ci VACINSOFT Folder Image: Ci VACINSOFT Folder Image: Ci VACINSOFT Folder Image: Ci VACINSOFT Folder Image: Ci VACINSOFT Folder Image: Ci VACINSOFT Folder Image: Ci VACINSOFT Folder Image: Ci VACINSOFT Folder Image: Ci VACINSOFT Folder Image: Ci VACINSOFT Folder Image: Ci VACINSOFT Folder
dup contents from: 26.11.2016 ame Type Size Modified Date arch Local Disk (C:) arch Local Disk (C:) arch Local Disk (C:) pe Size pe Size e folder e folder e folder e folder e folder	adup contents from: 26.11.2016 tame Type Size Modified Date if wCINSOFT Folder C:\WCINSOFT Folder C:\YS_YEDEX Folder f	v badup contents from: 26.11.2016 ▼ Name Type Size Modified Date C:\VASURSOFT Folder C:\VASURSOFT Folder C:\VASURSOFT Folder Folder C:\VasUrsoft Folder	w backup contents from: 26.11.2016 Image: Size Modified Date arch Local Disk (C:) Image: Size Civic Modified Date Image: Size Modified Date Image: Size Civic Modified Date Image: Size Modified Date Image: Size Civic Modified Date Image: Size Modified Date Image: Size Civic Modified Date Image: Size Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Image: Size Civic Modified Date Imag	ow backup contents from: 26.11.2016 Image: Size Modified Date arch Local Disk (C:) Image: Size Club City City City City City City City City	Ibackup contents from: 26.11.2016 Name Type Size Modified Date Image: Ci VACINSOFT Folder Image: Ci VACINSOFT Folder Image: Ci VACINSOFT Folder Image: Ci VACINSOFT Folder Image: Ci VACINSOFT Folder Image: Ci VACINSOFT Folder Image: Ci VACINSOFT Folder Image: Ci VACINSOFT Folder Image: Ci VACINSOFT Folder Image: Ci VACINSOFT Folder Image: Ci VACINSOFT Folder Image: Ci VACINSOFT Folder Image: Ci VACINSOFT Folder Image: Ci VACINSOFT Folder
ame Type Size Modified Date arch Local Disk (C:)	Name Type Size Modified Date ct/WGINSOFT Folder Image: Color to the state of	Name Type Size Modified Date arch Local Disk (C:) Image: Comparison of the comparison of the	Name Type Size Modified Date Image: C: VACINSOFT Folder Image: C: VACINSOFT Folder Image: C: VACINSOFT Folder Image: C: VACINSOFT Folder Image: C: VACINSOFT Folder Image: C: VACINSOFT Folder Image: C: VACINSOFT Folder Image: C: VACINSOFT Image: C: VACINSOFT Image: C: VACINSOFT Folder Image: C: VACINSOFT Image: C: VACINSOFT Image: C: VACINSOFT Folder Image: C: VACINSOFT Image: C: VACINSOFT Image: C: VACINSOFT Folder Image: C: VACINSOFT Image: C: VACINSOFT Image: C: VACINSOFT Folder Image: C: VACINSOFT Image: C: VACINSOFT Image: C: VACINSOFT Folder Image: C: VACINSOFT Image: C: VACINSOFT Image: C: VACINSOFT Folder Image: C: VACINSOFT Image: C: VACINSOFT Image: C: VACINSOFT Folder Image: C: VACINSOFT Image: C: VACINSOFT Image: C: VACINSOFT Folder Image: C: VACINSOFT Image: C: VACINSOFT Image: C: VACINSOFT Folder Image: C: VACINSOFT Image: C: VACINSOFT Image: C: VACINSOFT Folder Image: C: VACINSOFT Image: C: VACINSOFT Image: C: VACINSOFT Folder Image: C: VACINSOFT Image: C:	Name Type Size Modified Date arch Local Disk (C:) Period Image: CitACINSOFT Folder Polder pe Size Period Image: CitACINSOFT Folder Folder e folder e folder e folder Image: CitACINSOFT Folder Folder e folder e folder e folder Image: CitACINSOFT Folder e folder e folder e folder e folder Image: CitACINSOFT Folder e folder e folder e folder e folder	Name Type Size Modified Date C: VACINSOFT Folder C: VACINSOFT Folder C: VACINSOFT Folder C: VACINSOFT Folder C: VACINSOFT Folder C: VACINSOFT Folder C: VACINSOFT Folder C: VACINSOFT Folder C: VACINSOFT Folder C: VACINSOFT Folder
ame Type Size Modified Date C:WXINSOFT Folder c:WXCINSOFT Size Folder c:Wrogram Files/Firebird Folder c:Wrogram Files/Firebird Folder fol	Itame Type Size Modified Date c:\AKINSOFT Folder c:\AK_YPEEK Folder c:\Program Files\Firebird Folder e folder e folder e folder e folder e folder e folder	Name Type Size Modified Date © ciVASUNOFT Folder © ciVAS_VEDEK Folder © ciVaS_VEDEK Folder	Name Type Size Modified Date Image: CVAS_YEDEK Folder Image: CVAS_YEDEK </td <td>Name Type Size Modified Date Image: Citylogram Files/Firebird Folder Folder Image: Citylogram Files/Firebird Folder e folder Image: Citylogram Files/Firebird Folder e folder Image: Citylogram Files/Firebird Folder e folder Image: Citylogram Files/Firebird Folder e folder Image: Citylogram Files/Firebird Folder e folder Image: Citylogram Files/Firebird Folder e folder</td> <td>Name Type Size Modified Date © c:VACINSOFT Folder pe Size © c:VAS_VEDEX Folder e folder © c:VProgram Files/Firebird Folder e folder</td>	Name Type Size Modified Date Image: Citylogram Files/Firebird Folder Folder Image: Citylogram Files/Firebird Folder e folder Image: Citylogram Files/Firebird Folder e folder Image: Citylogram Files/Firebird Folder e folder Image: Citylogram Files/Firebird Folder e folder Image: Citylogram Files/Firebird Folder e folder Image: Citylogram Files/Firebird Folder e folder	Name Type Size Modified Date © c:VACINSOFT Folder pe Size © c:VAS_VEDEX Folder e folder © c:VProgram Files/Firebird Folder e folder
c:\WKINSOFT Folder pe Size c:\WS_YEDEK Folder c:\Program Files\Firebird Folder e folder e folder e folder	c:\AKINSOFT Folder c:\AS_YEDEK Folder c:\Program Files\Firebird Folder e folder e folder e folder e folder	Name Type Size Modified Date c:\WKINSOFT Folder pe Size c:\WS_YEDEK Folder e folder c:\Program Files\Firebird Folder e folder	Name Type Size Modified Date Image: ClAS_YEDEK Folder pe Size Image: ClAS_YEDEK Folder e folder e folder Image: ClAS_YEDEK Folder e folder e folder Image: ClAS_YEDEK Folder e folder e folder	Name Type Size Modified Date Image: ClAS_YEDEK Folder pe Size Image: ClAS_YEDEK Folder e folder e folder Image: ClAS_YEDEK Folder e folder e folder Image: ClAS_YEDEK Folder e folder e folder Image: ClAS_YEDEK Folder e folder e folder Image: ClAS_YEDEK Folder e folder e folder	Name Type Size Modified Date © ci\AKINSOFT Folder pe Size © ci\AS_YEDEK Folder e folder © ci\Program Files\Firebird Folder e folder
c:\WKINSOFT Folder pe Size c:\WS_YEDEK Folder c:\Program Files\Firebird Folder e folder e folder e folder	c:\AKINSOFT Folder c:\AS_YEDEK Folder c:\Program Files\Firebird Folder e folder e folder e folder e folder	C:\VKINSOFT Folder C:\VS_YEDEK Folder C:\Vprogram Files\Firebird Folder e folder e folder e folder e folder e folder e folder	Image: Comparison of the second se	Image: Constraint of the second of the se	c:\VAXINSOFT Polder c:\VS_YEDEK Polder c:\Vs_Yrogram Files\Firebird Folder c:\Vrogram Files\Firebird Folder
c:VAS_YEDEK Folder folder folder folder folder folder folder	C:\AS_YEDEK Folder C:\Program Files/Firebird Folder E Folder E Folder E Folder E Folder E Folder E Folder	C:\AS_YEDEK Folder pe size C:\Program Files\Firebird Folder e folder e folder e folder e folder e folder e folder e folder	Image: City System Polder Polder Image: City Program Files Virebird Folder e folder Image: City Program Files Virebird Folder e folder Image: City Program Files Virebird E folder e folder Image: City Program Files Virebird E folder e folder Image: City Program Files Virebird E folder e folder	C:\AS_YEDEK Polder C:\Program Files\Firebird Folder e folder e folder e folder e folder e folder e folder e folder e folder e folder e folder	C: \AS_YEDEK Folder c: \Yrogram Files\Firebird Folder e folder e folder e folder e folder
I c:VAS_YEDEK Folder e folder e folder e folder	ctVS_YEDEK Folder e f	C:\V5_YEDEX Folder C:\Program Files\Firebird Folder e folder e folder e folder e folder	Image: ClyProgram Files/Firebird Folder Image: ClyProgram Files/Firebird Folder Image: ClyProgram Files/Firebird Folder Image: ClyProgram Files/Firebird Folder Image: ClyProgram Files/Firebird Folder Image: ClyProgram Files/Firebird Folder Image: ClyProgram Files/Firebird Folder Image: ClyProgram Files/Firebird Folder Image: ClyProgram Files/Firebird Folder Image: ClyProgram Files/Firebird Folder Image: ClyProgram Files/Firebird Folder	C:VAS_YEDEK Folder C:VProgram Files/Firebird Folder e folder e folder e folder e folder e folder e folder e folder e folder	c:\A5_YEDEK Folder c:\Program Files\Firebird Folder e folder e folder e folder e folder
e folder	e folder e folder e folder	e folder e folder e folder	e folder e folder e folder e folder	e folder e folder e folder e folder e folder	e folder e folder
	e folder e folder	e folder e folder	e folder e folder e folder	e folder e folder e folder e folder	e folder
- 611	e folder	le folder	e folder e folder	e folder e folder e folder	
e tolder			e folder	e folder e folder	le folder
e folder		le folder		e folder	
e folder	le folder		e folder		e folder
e folder		e folder		a folder	e folder
	e folder		Select All Deselect All e folder		
t All Deselect All e folder		e folder		Select AI Deselect AI Deselect AI bt Document 6 KB	e folder
e folder		e folder		e folder	e folder
	e folder		a fuller		

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.