Operation "Oil Tanker"

The Phantom Menace

panda

Operation Oil Tanker: The Phantom Menace.

Everything started on a cold January day in a coastal town in the North East of England, an area with a strong presence of petrochemical companies.

The day began normally in one of these companies, a firm specializing in, among other things, maritime oil transportation. Let's call this company "Black Gold".

John, the head of Black Gold's IT Department knows that we live in a dangerous world, and that companies face thousands of cyber-attacks every day. And although Black Gold is not included in the Fortune 1000 company list, John knew that taking all possible safety precautions is a must and that, in addition to having a corporate antivirus, they must maximize all other security measures.

That's why when given the opportunity to take part in a pilot program involving a new service that monitors all applications running on endpoints, reporting the security status of the network and providing forensic information in the event of infections, he didn't think twice. After completing a series of controlled tests, John decided to deploy the small agent across the company's network October 2013.

The information he received during the first three months helped to identify computers at risk where vulnerable applications were found. Apart from that, nothing worth mentioning really happened.

Thanks to John, Black Gold joined a high IT security pilot program.

One day, however, while Susan, a secretary with more than 20 years of experience at Black Gold, was checking her email as she did every Monday morning, she came across an email message with an attached document.

The document appeared to be a PDF file of approximately 4MB in size, with information about the oil market. Nothing suspicious. Besides, the message in question had gone through every security filter in place. Neither the mail server antivirus nor the antivirus on her workstation had found anything anomalous in it.

Susan double-clicked the attachment. A blank PDF opened. "This must be a mistake. I hope they realize it and send us the correct file again," Susan thought, moving on to the next unread message.

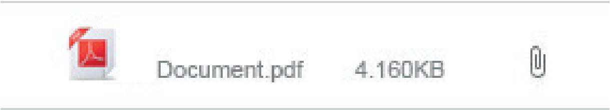
Meanwhile, 1,700 km away from Susan's computer, an alarm was triggered. An unknown threat had just been detected and blocked when it tried to steal credentials from Susan's computer and send them out.

Today, most computer threats are designed to steal information from target systems, so this just looked like thousands of cases we examine in the laboratory every day. However, it caught our attention that no antivirus engine had been able to detect it, although this shouldn't be so surprising if you take into consideration that every day over 250,000 new malware files are put in circulation. There was something really unique about this threat: it didn't use any kind of malware. That's why we decided to call it the 'Phantom Menace'.

Susan just clicked twice, and the 'Phantom Menace' was triggered.

Attack analysis

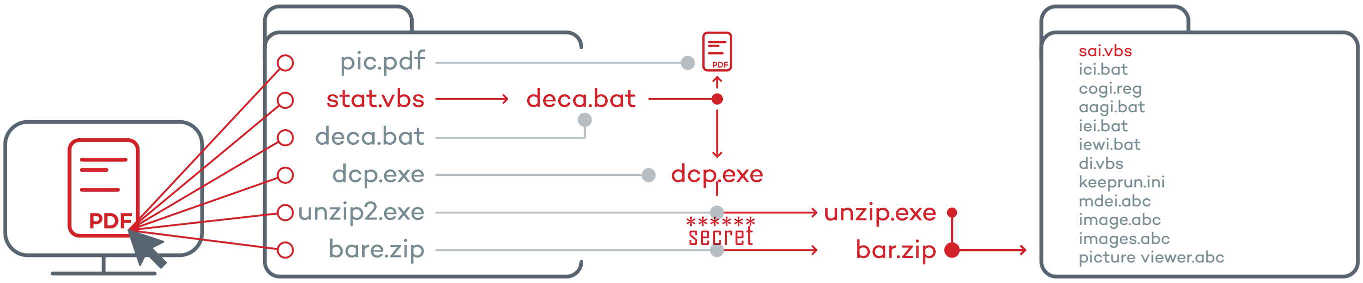
The file that Susan received and opened looked like this.



Document.pdf 4.160KB

It actually was an executable file that used the icon typically used by Adobe Acrobat Reader documents to trick users.

The figure below illustrates the execution flow:



The file is just a self-extracting file. Once run, it creates a folder and extracts six files into it. It then runs one of them –stat.vbs– and does not take any more actions.

There is no malicious activity, so the file goes unnoticed by behavior-based detectors. The stat.vbs file simply runs another file –deca.bat– in the background.

This file in turn opens the pic.pdf file (the blank PDF document that opened on Susan's computer) and runs a file called dcp.exe, a free tool to encrypt files.

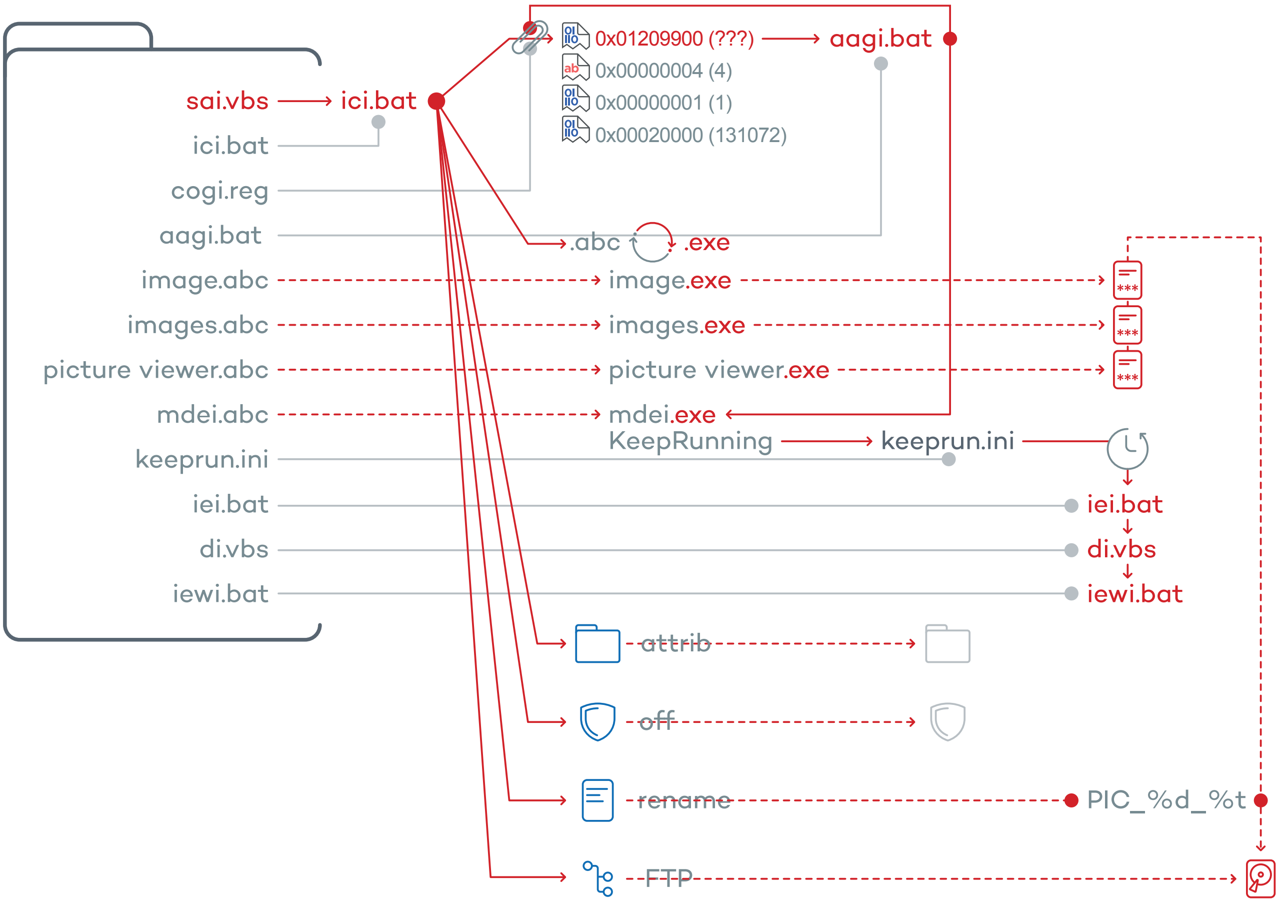
This utility is used to decrypt the following two files:

unzip2.exe → unzip.exe

bare.zip → bar.zip

Next, it uses the unzip.exe program to extract the content of the bare.zip file (12 files) into a different folder. Then, it runs one of the files: sai.vbs.

None of these actions are anomalous, and actually are very different from what we normally see in other types of attacks. Here is where the second part of the attack begins:



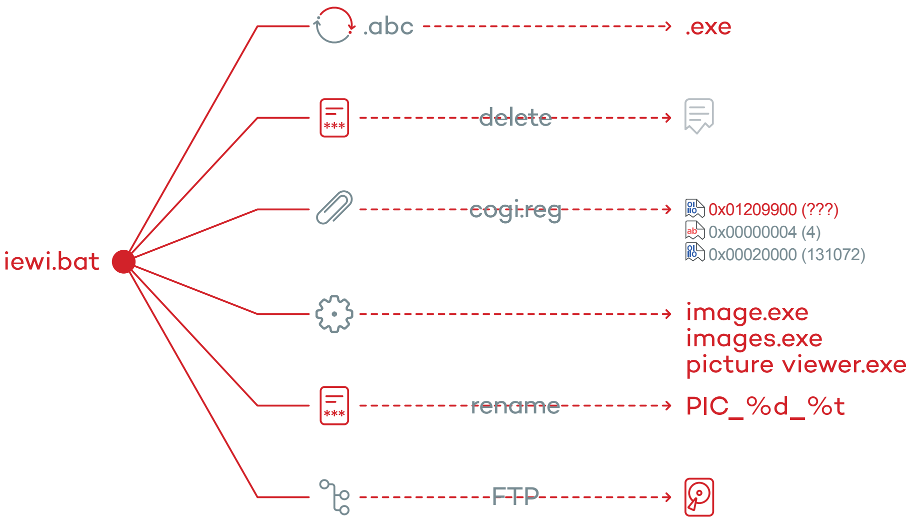
The .vbs file runs a .bat file that modifies the Windows registry to ensure that a file called aagi.bat is run every time the system starts. Then, it makes a copy of the four files with the extension .abc, and changes their extension to .exe. These are all legitimate applications that anybody could use: the first three are designed to collect the credentials (user names and passwords) stored in the local mail client and Internet browser, and save them to a text file.

The fourth one is an application designed to run another application every 'x' seconds. This is very useful for computers that need to run an application at all times, like a browser or any other specific software, so that if the application closes unexpectedly for some reason it will open again. In this case the application is configured to run another .bat file every 3,600 seconds (every hour).

Then, the ici.bat file uses the ATTRIB system command to hide the two folders it created, disables the Windows firewall, and renames the text files containing the credentials to PIC_%d_%t, where %d is the current date and %t the current time. This is done to indicate when the information they contain was obtained.

Finally, it uses the FTP command to upload those files to an external FTP server controlled by the attackers.

Additionally, it runs the file iei.bat every hour, which basically takes the following actions:



It renames the .abc files back to .exe, in case they were deleted. It then deletes all the text files with credentials that were already uploaded to the FTP server, restores the Windows registry key in case it was deleted, runs the applications designed to collect credentials, renames the resulting files and uploads them to the FTP server.

As you can see, no malware is ever used in the attack, the hack makes use of legitimate tools and different scripts to perform the aforementioned actions.

But, is this type of attack really effective? As mentioned before, no antivirus was capable of detecting it. Furthermore, its peculiarities seem to indicate that the proactive protection layers included in most antivirus solutions would not be able to detect its apparently harmless behavior.

This was confirmed when we accessed the FTP server that the stolen data was sent to, and found that the oldest files dated back to August 2013. That is, the attack had been underway for almost six months completely undetected.

A targeted attack?

Once we accessed the FTP server, the first thing we did was look for credentials belonging to Black Gold, since, despite being able to neutralize the attack on Susan's computer, another employee could have fallen victim to it. The result was negative, no credentials had been stolen from the company.

However, we were surprised by the large number of files stored on the FTP server: over 80,000 text files with stolen credentials from other firms. **This didn't look like a targeted attack**, where the number of victims is usually low.

However, after opening three files at random, we found that they belonged to three companies all in the same industrial sector that Black Gold belongs to.

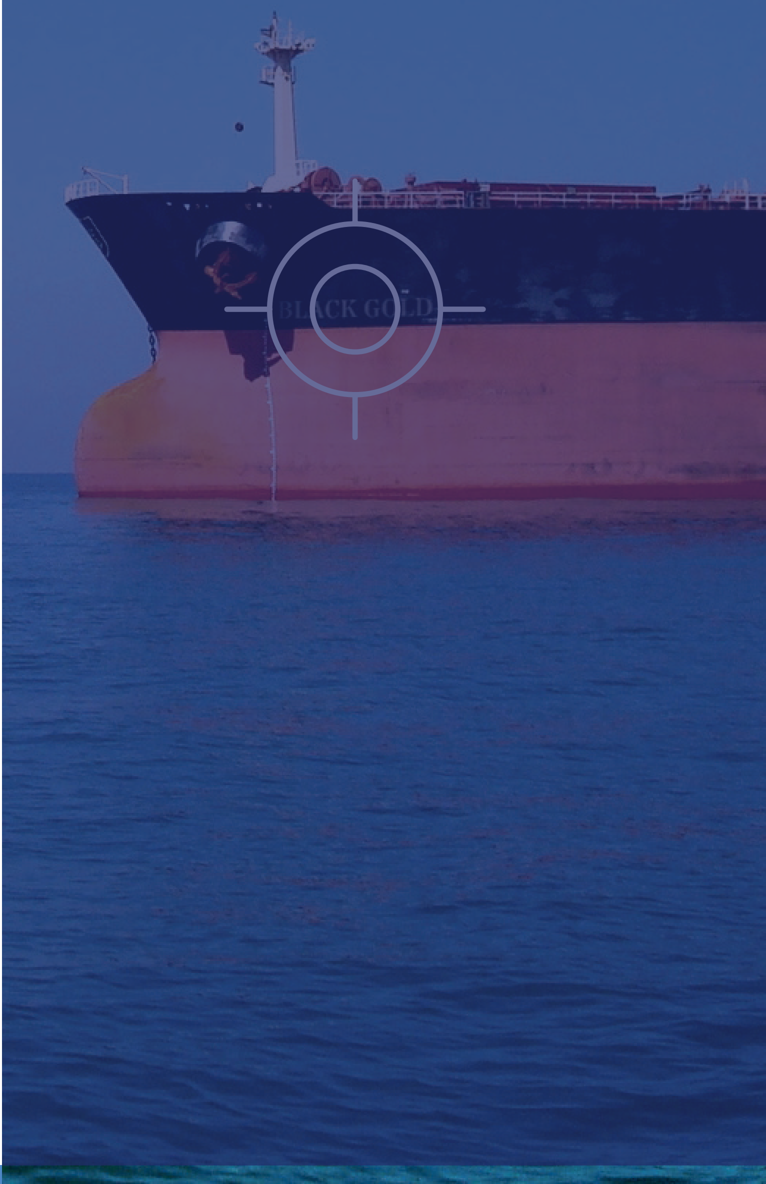
As mentioned in the previous section, the attack took place recurrently every hour. This means that stolen credentials were sent to the FTP server every hour. We discarded duplicate files and ended up with 860 unique files.

That was still too many files for a targeted attack. The only thing left to do was manually process all these files and try to identify the victims.

The files belonged to some ten companies, all of them in the oil and gas maritime transportation sector.

It was clear that the hack was indeed a targeted attack, but we still didn't know what the attackers were really after, what their final objective was.

What didn't seem a targeted attack at first, ended being a whole conspiratorial plot against the sector.



Nigeria, scams and oil

The so-called Nigerian scams have been a constant presence on the Internet since its inception, and even before that, when fraudsters used postal mail to defraud victims.

In the most popular one, the scammer passes themselves off as an important figure in the Nigerian government or some other institution, and contacts the victim offering them a share in a large sum of money that they want to transfer out of the country.

However, the Nigerian scam industry is large and varied. Some variants are almost unknown and affect all kinds of sectors, including the oil industry.

The Nigerian town of Bonny is well-known in oil production circles as the oil produced there, known as Bonny Light Crude Oil (BLCO), has a very low sulfur content, which makes it a highly desired grade for its low corrosiveness.

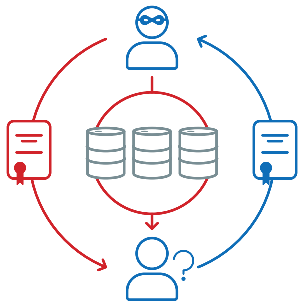
The fact that this particular type of oil is in such high demand has given rise to a particular type of scam aimed at oil brokers, individuals who arrange transactions involving crude oil between buyers and sellers.

In Nigeria, every gas and oil transaction is supervised by the NNPC (Nigerian National Petroleum Corporation), a government-owned company. Anybody who wants to trade with oil in Nigeria must be registered with the NNPC.

In short, the scam works like this: the scammer contacts a broker/middleman and offers them a large amount of BLCO, one to two million barrels, at a very competitive price.

If the potential buyer is interested, they will ask for documentary evidence that the product exists (Proof of Product). There are different types of documents that can be provided: a quality certificate, a certificate of origin, a cargo manifest, or the letter of ATS (Authority to Sell) issued by the NNPC.

To close the deal, the buyer must pay a significant amount of money -from $50,000 to $100,000- in advance. However, once they pay the money they are met with the nasty surprise that there is no oil.



The weakest link in the scam is the documentation that the scammer must provide to convince the buyer. Even though all of these documents can be forged, the fraudster runs the risk of being discovered by the broker.

To make it more plausible, scammers attempt to use real documents so that if the broker wishes to check their legitimacy, they will see that they are real.

However, how difficult is it to obtain these documents? It is very complicated. The only way to do it is from companies in the sector. Oil transportation companies, for example. This was just a theory, at that time we didn't have any evidence to prove that that was the objective of those responsible for the 'Phantom Menace' attack.

Is it possible to know who is behind the attack?

In most cases, getting to know who is behind a cyber-attack is very complex, sometimes impossible.

In this case we were fairly pessimistic. To make it worse, the fact that no malware had been used in the attack ruled out the possibility of finding a signature to examine. However, there was a weak spot in the attack: the FTP connection used to send out the stolen credentials.

The information was transmitted using the FTP command, and as that command was called by one of the scripts, it was possible to see the connection used, from where it was established and the credentials used. The FTP server belonged to a free service that the attacker had signed up to, so we were able to access it and see the information entered when opening the account. Yes, we were aware that the information would probably be false, but it was still worth checking.

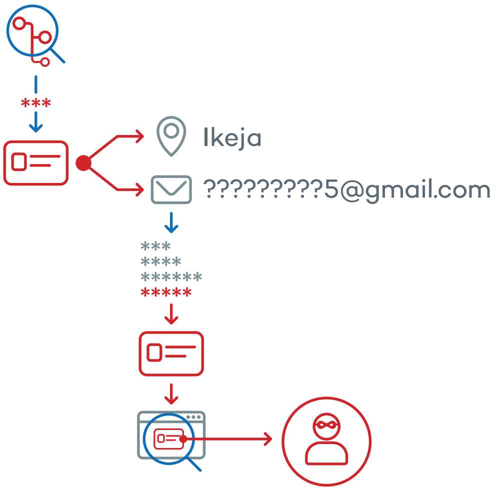
The name used was false; googling it returned zero results. The country selected was the United States, which could be false as well. Then we had a look at the city information. The name in this field was unknown to us: "Ikeja".

It turns out that Ikeja is the name of a suburb in Lagos -the capital city of Nigeria-, also known as the "Computer Village" as it hosts the nation's largest market cluster for technology products. This information could also be false, but the fact that whoever opened the account was familiar with that name meant that they were from Nigeria themselves or knew the country very well.

Then came the email address. This was the only element that we knew for sure had to be real and valid, as it is the address at which users receive the service activation message, password reset messages, etc. In this case it was a Gmail address: *********5@gmail.com

The password was unknown, they hadn't used the same one as for the FTP service. We took the 9 characters that made up the email address and started combining them to see if we could form an alias, a first name, a last name or similar. **And we got it**.

We googled what looked like a first name and last name and got a hit. It was the name of a person with Nigerian nationality and Twitter, Facebook and LinkedIn accounts, which allowed us to obtain some more information about him. All those accounts belonged to a person living in... Ikeja and who is the owner of a goods transport company.



Too many coincidences. So, even though all the evidence seems to indicate that this is the person responsible for the attack, there is no way for us to prove it. It would require the police to launch an investigation and obtain information about the FTP connections, etc., in order to get the IP address of the person who signed up to the service and find the culprit.

Conclusion

With all the information we had in our hands, the idea of what to do next was clear: inform the police so that they could start an investigation and apprehend whomever was responsible for the hack.

Since one the affected companies was from Spain, we contacted the Spanish Civil Guard, a police force that we have collaborated with in the past and which has a very good reputation in the fight against cyber-crime. Unfortunately, they face a difficult-to-solve problem: to start an investigation they need a victim who reports the crime. It looks simple, but it isn't: **none of the victims of this attack is willing to report it**.

Why? If our theory is correct, the information stolen from these companies has not been used against them, but to defraud other people, oil buyers. It is for that reason that the companies which have had their credentials compromised prefer not to report the attack for fear of having their name in the spotlight. They prefer to keep a low profile, change their credentials and continue to operate just as if nothing had happened.

Some countries have laws that force companies to report every hacking intrusion where information is stolen. However, that obligation is usually limited to incidents in which the stolen information belongs to a third party (customers, partners, etc.). In this case, the stolen credentials belonged to the company under attack, which therefore is not forced by law to report the theft.

We started this article by calling this case 'The Phantom Menace', due to the nature of the attack and the absence of malware to perpetrate it. Continuing with the homage to Star Wars, it is time to move on to 'The Force Awakens': all major companies must awake to their vulnerability and realize that absolute security doesn't exist and behavior-based protection is limited.

They need to go one step further, performing regular audits in order to assess and address potential weaknesses in their network security. Despite traditional security solutions are still a necessity, they are no longer enough. It is important to understand that our defense systems must adapt to the level of attack received, and so it is necessary to implement new protection strategies that give organizations total control and visibility over their networks.

The companies like Black Gold usually prefer not to demand this kind of attacks in order keep them in anonymity.

This article in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Panda Security.

© Panda Security 2015. All Rights Reserved.