APT

OceanLotus (APT-C-00)

3—Year Cyber Space Threat

SkyEye
天眼实验室

Abstract

- Since April 2012, a hacker group performed an organized, well planned, targeted, long-term and persistent campaign against relevant important organizations of Chinese government, research institutes, maritime agencies, marine construction and shipping companies, etc. We named the responsible group as OceanLotus.
- OceanLotus planted sophisticated trojans to the target organizations within Chinese territory through spear phishing and water holing attacks, combined with various means of social engineering.
- More than 100 OceanLotus trojan samples were captured. They affected targets in over 29 provincial administrative regions throughout China and 36 other countries. Among them, 92.3% were in China mainland. Beijing and Tianjin were the two most affected regions.
- In order to hide the source of attacks, OceanLotus used at least 35 C2 (also known as C&C, which is an abbreviation of Command and Control) domain names and 19 related IP addresses in six countries, with servers distributed in more than 13 different countries around the world.
- After February 2014, OceanLotus entered its active stage of attack, and launched the largest round of spear phishing attack in May 2015. In May and September of 2014, and in January 2015, the group launched multi-rounds of targeted water holing attacks by hacking web sites of government agencies.
- OceanLotus used four different types of customized trojans which became more and more sophisticated to gain access of target systems.
- The attacks from OceanLotus were featured by a long attack cycle (lasting over 3 years), well resourced, specifically selected targets, complex techniques and precise means of social engineering, which all indicated that the group is not an ordinary hacker team, but is likely to be a highly professional, organized and state-sponsored APT group.

Key words: OceanLotus, APT, spear phishing, water holing

CONTENTS

Overview of OceanLotus

Since April 2012 till today, a certain hacker group performed an organized, well planned, targeted, long-term and persistent campaign against relevant important organizations of Chinese government, research institutes, maritime agencies, marine construction and shipping companies, etc. The group mainly spread sophisticated trojans to targeted groups within the Chinese territory combined with various means of social engineering, and secretly controlled computer systems of government personnel, contractors and industry experts and stole confidential information through spear phishing and water holing attacks.

Based on the attack characteristics of this group, we named the group as OceanLotus.

The first customized trojan related to OceanLotus was captured in April, 2012. In the following 3 years, we successively captured more than 100 OceanLotus trojan samples of 4 different types that related to this group, the infected target spread all over 29 provincial administrative regions throughout China mainland and 36other countries. In addition, in order to hide the source of attack, the group registered at least 35 C2 (also known as C&C, which is an abbreviation of Command and Control) domain names used as a remote control of infected systems and 19 related IP addresses in six countries, with servers distributed in more than 13 different countries around the world.

From the perspective of the history of the OceanLotus attack, the following points in time and events are worth attention:

1) In April 2012, the Trojan associated with the group was found for the first time. The penetration attack organized by OceanLotus began during this time. However, during the following two years, OceanLotus was not very active.

2) In February 2014, OceanLotus began to launch targeted attacks to Chinese domestic targets by spear phishing attack. OceanLotus entered its active stage, and launched persistent attacks against multiple targets in China in the following 14 months.

3) In May 2014, OceanLotus launched a large-scale spear phishing attack to an authority marine research institute in China, and reached the peak of spear phishing attacks in the past 14 months.

4) Also in May 2014, OceanLotus tampered and injected trojan program in an

official website of a marine construction institution in China, which formed the first round of large-scale water holing attacks.

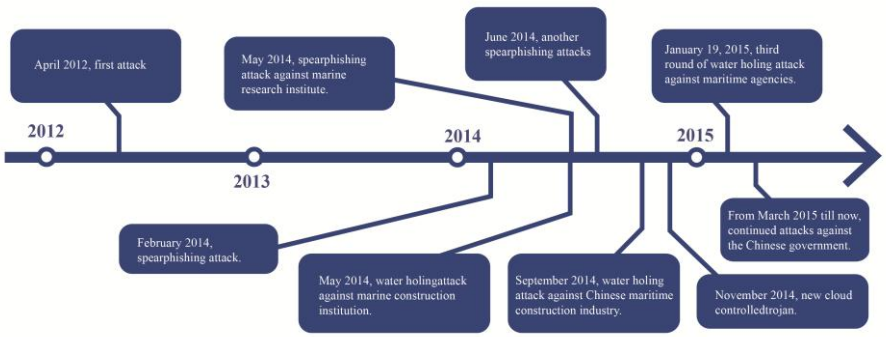
5) In June 2014, OceanLotus began to launch a large amount of spear phishing attacks against related organizations and groups of Chinese fishery resources.

6) In September 2014, OceanLotus launched water holing attacks against the related industries of Chinese waters construction, which formed the second round of large-scale water holing attacks.

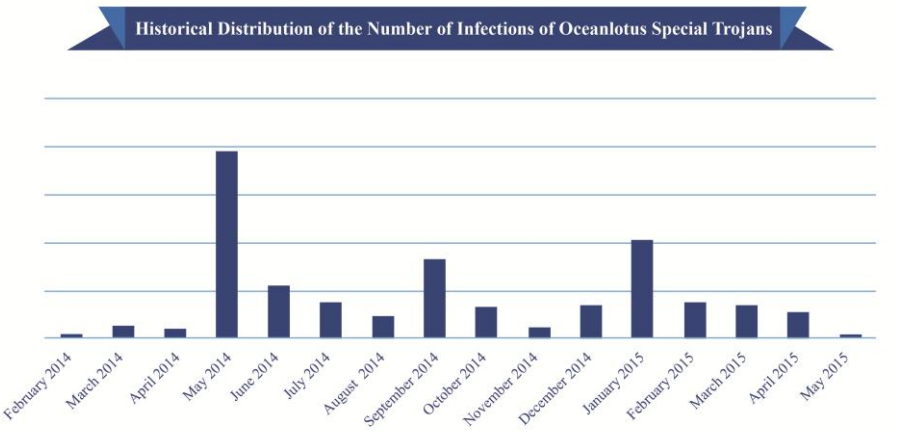
7) In November 2014, OceanLotus began to use a cloud controlled trojan which was more aggressive and well concealed, to continuously launch attacks against targets within China.

8) In January 19, 2015, OceanLotus injected the trojan programs into website of a maritime agency of Chinese government, which formed the third round of large scale water holing attacks.

9) From March 2015till today, OceanLotus continuously carries out attacks against other agencies affiliated to the Chinese government.



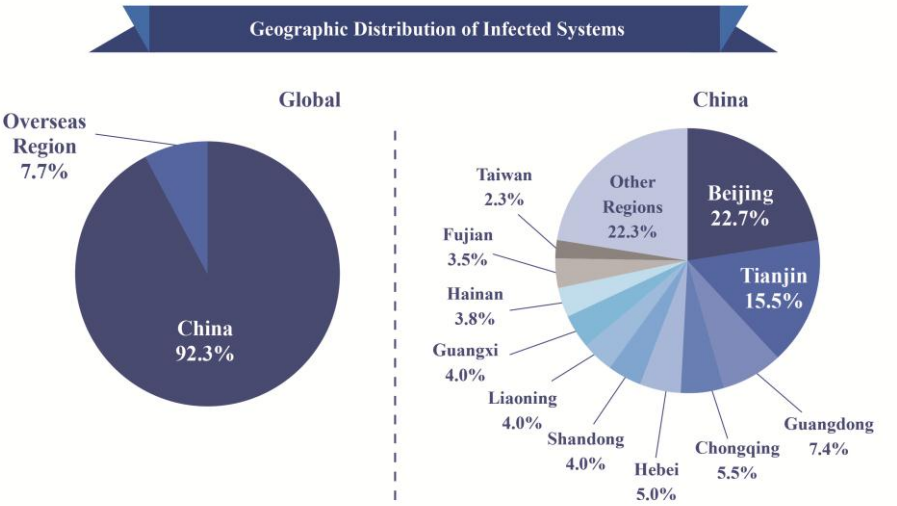
By tracking and conducting forensics of years of attack activities conducted by OceanLotus, we have confirmed a large number of victims. The figure below is the distribution trend of the number of computers that infected by OceanLotus sophisticated trojans every month from February 2014 until now.



Historical Distribution of the Number of Infections of OceanLotus Sophisticated Trojans

Feb 2014, Mar 2014, May 2014, June 2014, July 2014, Aug 2014, Sep 2014, Oct 2014, Nov 2014, Dec 2014, Jan 2015, Feb 2015, Mar 2015, Apr 2014, May 2015

From the view of geographic distribution, the number of infected system in China is 92.3% of total global infected targets. Beijing accounts for the most number of infected targets, which is 22.7%, and Tianjin is the second, which is 15.5%.



The figure below is the geographic distribution of the number of infected targets of the Trojan.

Our research shows that the technology of their early stage trojan was not complicated, and was easy to detect and remove. But after 2014, OceanLotus started to use a series of complex attack technologies, including file camouflage, random encryption and self-destruction, etc. to fight against the security software, which increased the difficulty of detection and capture. Furthermore, after November 2014, OceanLotus sophisticated Trojan started to use cloud control technology, which greatly increased the risk and uncertainties of the attack and difficulties of killing the trojans

In conclusion, the attacks from OceanLotus were featured by a long attack cycle (lasting over 3 years), well resourced, specifically selected targets, complex techniques and precise means of social engineering, which all indicated that the group is not an ordinary hacker team, but is likely to be a highly professional, organized and state-sponsored APT group.

OceanLotus Attack Techniques

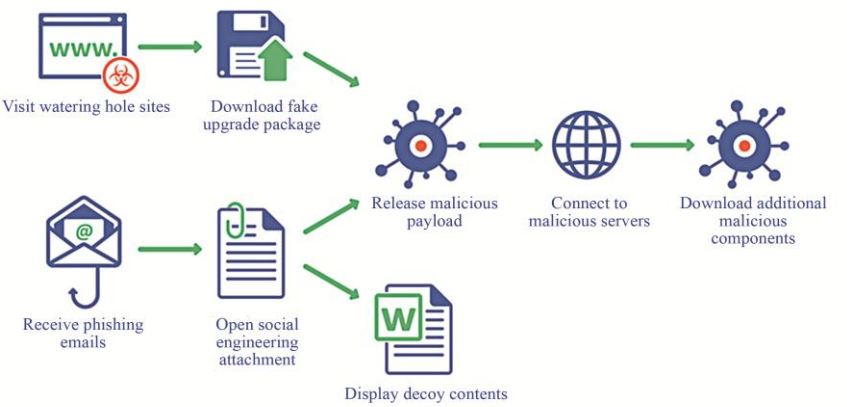
Summary of Attack Techniques

OceanLotus mainly performs attacks through two techniques: Spear Phishing and Water holing.

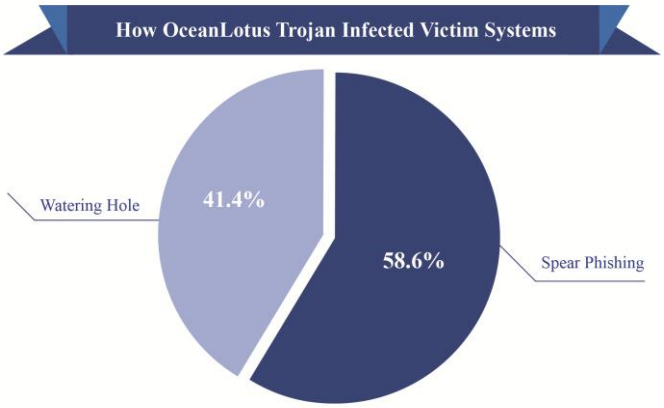
Spear phishing is a spoofing fraud attack that targets a specific organization, seeking unauthorized access to confidential data. The common method is to send emails to the target with a trojan as attachment, luring the victim to open the attached trojan.to execute malicious code.

Water holing refers to the kind of attacks that hackers insert malicious code in legitimate websites for the explicit purpose of attacking the targeted visitors, whose online activities may be carefully analyzed to obtain their online surfing habits.

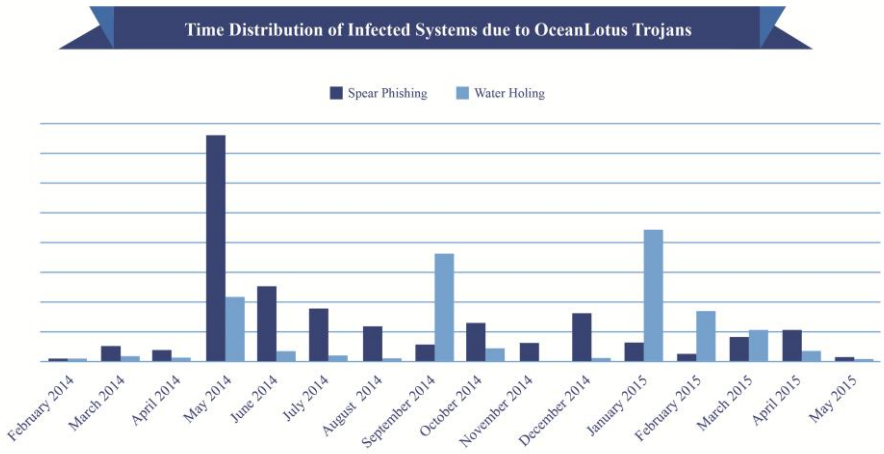
Basic attack methods of OceanLotus via spear phishing and water holing are demonstrated as followed.



As for the victims up to now, 58.6% suffered spear phishing attack and 41.4% suffered water holing attacks.



The chart below is the time distribution of infected systems due to spear phishing or water holing attacks. The peak of spear phishing appeared on May, 2014 and peak of water holing attacks came on September 2014.



Spear Phishing

OceanLotus will carefully select the target organization first and send malicious emails to employee of the target organization after collection of email information. The victims' computers will get infected if the malicious attachment is clicked. Once the trojan and C2 server get connected, the computer system will be controlled by OceanLotus. Based on the monitoring of SkyEye, OceanLotus has conducted spear phishing since Feb, 2014, with new victims increasing each month.

OceanLotus usually sends emails attached with ".exe" executable programs disguised as Office Word documents during spear phishing. To improve its success rate, the attacker often names the attached document with a hot topic or

issues related to personal interest. Some document names looks closely related with the targeted organization, which clearly shows features of an APT attack. Two samples are as following.

1）Riots in Urumqi Related Spear Phishing

On May 22, 2014, Riot took place in Urumqi, Xinjiang. We captured phishing emails with attachment named “Latest Pictures & News about Riot in Xinjiang.jpg.exe” on May, 28.

2）Civil Servant Salary Reform Related Spear Phishing

During 2014 and 2015, Chinese government released Civil Servant Salary Reform Scheme, which directly impacted government employees. With 7 million civil servants in China, salary reform of civil servants has been a hot topic among government employees for a long time.

On Sept.9 2014, we captured phishing emails with a malicious attachment named “Salary System and Special Allowance”. On Nov. 5, 2014, A phishing email with a malicious attachment named “Notice on Salary Reform Policy” was also captured. Meanwhile, other similar phishing emails were captured as well. Based on analysis, all the phishing emails were spear phishing email sent by OceanLotus targeting government employees.

Based on the follow-up analysis of phishing emails by OceanLotus, we found some regular pattern among attachments used ---- email content and names of attached files are closely related with marine resources, construction of marine enterprises, Chinese government and research institutes. Some of the files are as followed.(organization names and sensitive content are replaced with “*”).

Related file name
关于国家***研究中心工程建设的函.exe
国家**局的紧急通报.exe
最新新疆暴动照片与信息.jpg.exe
本周工作小结及下周工作计划.exe
厅关于印发《2014 年应急管理工作要点》的通知.exe
2015 年 1 月 12 日下发的紧急通知.exe
商量好的合同.exe
部关于开展 2015 年调查工作的通知.exe

Related file name
Letter on Construction of State ***Research Center.exe
Urgent Notice from State Bureau of**.exe
Latest Pictures and News about Riot in Xinjiang.exe
Weekly Summary & Next Week Plan.exe
***Department Notice on 2014 Event Reponses Mnagement.exe
Urgent Notice on Jan, 12, 2015.exe
Agreed Contract.exe
Notice from XX Ministry on 2015 Review.exe

Some trojan email attachments by OceanLotus will use a long extension name to exploit file name display mechanism of Windows OS. Due to the long extension, the real ".exe" executable extension of files will not be displayed automatically. Thus, for most of file receivers, files are recognized as Office documents and clicked to view.

Statistics shows that spear phishing by OceanLotus is characterized by timeliness and periodicity. Most spear phishing attacks are captured during working days and few spear phishing on weekends (less than 1/5 of workdays).

Water Holing

When setting up watering holes in attacks, OceanLotus adopts two main methods after taking control of the related Web server: the first one is they replace the normal software installation package needed or tempt people to download the forged normal software (Adobe Flash) upgrades in order to get malicious program executed in target's systems; the second one is they tamper links of Web site which will redirect to machine under attacker's control and entice target to download malicious executables.

The lifecycle of watering hole attacks is usually short to avoid detection. After completing attacks within 3 to 5 days, OceanLotus will delete or recover the tampered contents. Due to that reason, it is very difficult to reconstruct the watering hole attack scenarios.

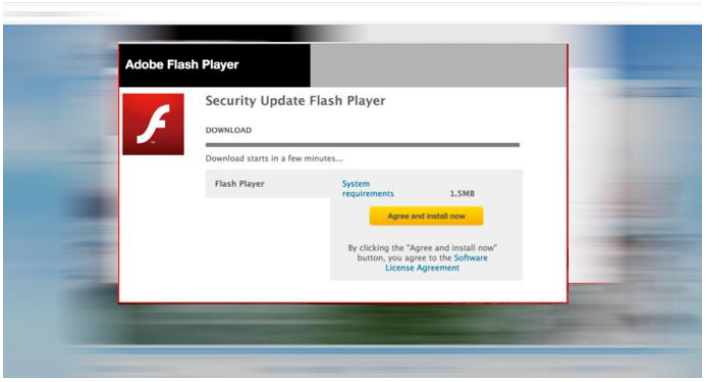
The following two examples that have been reconstructed with technical methodologies are provided to illustrate typical watering hole attacks:

Example A:

First, they illegally gained control of file exchange servers through invasion. Then they bundled normal installation packages of two normal applications used

for instant messaging and a certificate driver with their trojan code. After that, when users downloaded and opened these applications, they were \infected by the trojans. Attackers also inserted malicious script code in the pages of tampered servers. When visiting these sites, users were prompted to update Flash software, but these sites actually provided Flash upgrade packages with malicious program injected. Users will get infected by trojans if they download and open these packages.

The next picture shows when users visiting watering hole sites, forged Flash upgrade packages by JS code prompted users to update.

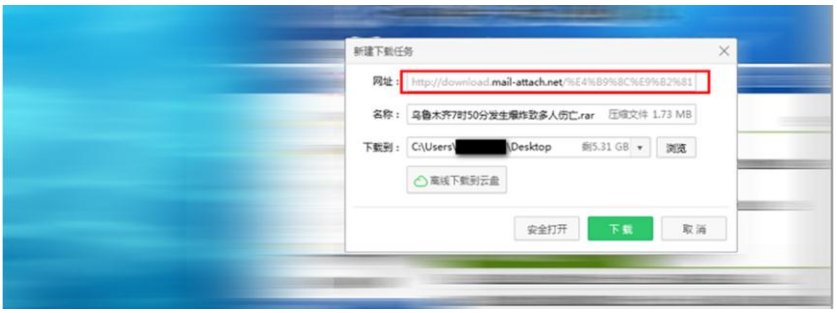


Additionally, OceanLotus's specialty is also reflected in that they will identify the operating system of visitors. They will send various malicious packages targeting different systems according to system information returned by client-sides. When using Windows system, users will be promoted to download upgrade files called "install_flashplayer.exe"; when it comes to Safari , the malicious program is named "install_flashplayer_mac.zip" which is a Mac OS system application.

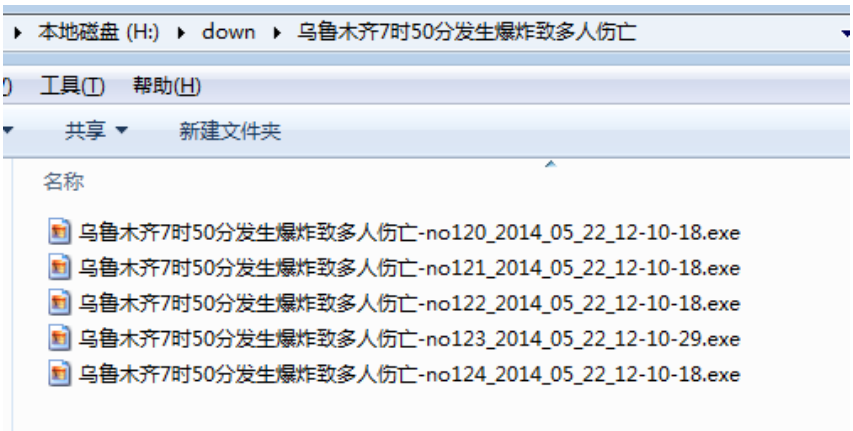
Example B:

This compromised website is a government site that provides materials downloads for marine researchers and experts, research project press and related issues notices. After breaking into this site, OceanLotus falsified its routine. When visiting this site, users were redirected to another website controlled by attackers and promoted to download a file looked like a news report. For example, the day after the Xinjiang terrorist attack, related notices and news appeared on the website. When users downloaded packages named "Urumqi's explosion on 7:50 caused many casualties .rar", they were infected by particular trojans developed by OceanLotus.

The following picture shows when users clicked notice links, they are prompted to download a certain report.



download.mail-attach.net in the dialogue box is the server controlled by OceanLotus. If we unzip the file named “Explosion in Urumqi at 7:50 resulted in many injuries and deaths”, we can see the “.exe” executable file with the icon of JPG pictures. Clicking of the file will result in the infection of the victim system,



Meanwhile, some malicious programs for spear phishing are found under the same watering hole file directory, which can prove the watering hole attack and previous spear phishing were conducted by the same group. Below are some files listed.

SkyEye Labs has reached a conclusion about attacking methods after tracked analyzing OceanLotus’ watering hole attacks. When OceanLotus has

opportunities to break into servers related with targets, they will replace normal applications for downloads by forged application updating packages.

The next table shows malicious files that have appeared in some watering hole servers.

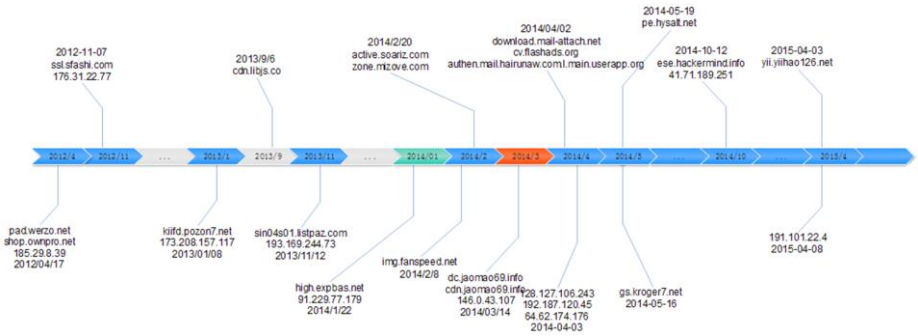
文件名	文件 MD5
install_flashplayer.exe	7e68371ba3a988ff88e0fb54e2507f0d
rtx.exe	0529b1d393f405bc2b2b33709dd57153
sinopec.exe	9fea62c042a8eda1d3f5ae54bad1e959
报表插件安装程序.exe	486bb089b22998ec2560afa59008eafa
USBDeview.exe	b778d0de33b66ffdaaf76ba01e7c5b7b
DSC00229.exe	53e5718adf6f5feb2e3bb3396a229ba8
install_flashplayer13x37.exe	d39edc7922054a0f14a5b000a28e3329
NetcaEKeyClient.exe	41bced8c65c5822d43cadad7d1dc49fd

File Name	File MD5
install_flashplayer.exe	7e68371ba3a988ff88e0fb54e2507f0d
rtx.exe	0529b1d393f405bc2b2b33709dd57153
sinopec.exe	9fea62c042a8eda1d3f5ae54bad1e959
报表插件安装程序.exe	486bb089b22998ec2560afa59008eafa
USBDeview.exe	b778d0de33b66ffdaaf76ba01e7c5b7b
DSC00229.exe	53e5718adf6f5feb2e3bb3396a229ba8
install_flashplayer13x37.exe	d39edc7922054a0f14a5b000a28e3329
NetcaEKeyClient.exe	41bced8c65c5822d43cadad7d1dc49fd

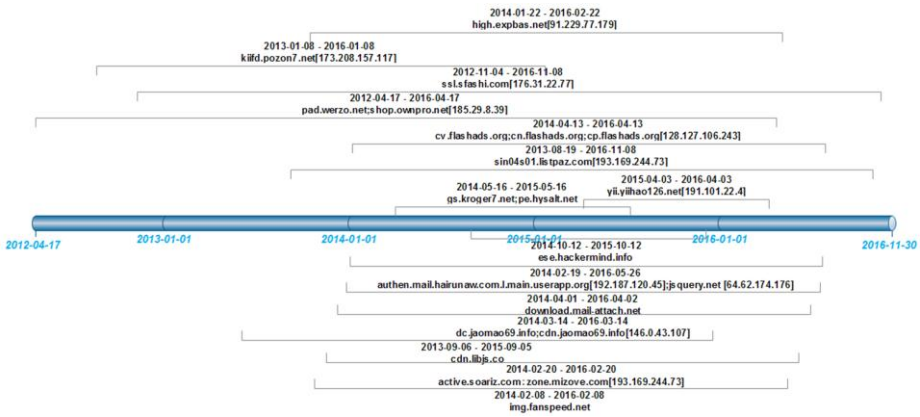
Based on the analysis of water holing attacks launched by OceanLotus, the number of infections on Monday and Tuesday are the largest for the week. SkyEye Labs suggests the possible reason is that OceanLotus has studied government and research institute personnel's habits of surfing the Internet. Due to the high possibility of organizational information leakage, the cycle of watering hole attack is usually less than 3 days. And to make such short-period attacks more effective, OceanLotus has to take the government staff's habits visiting websites into consideration. Since most government and research institute staff has the habit of reading major internal news and notices on Monday and Tuesday, OceanLotus has achieved great effect in launching attacks on Monday and Tuesday.

Domain Name Change

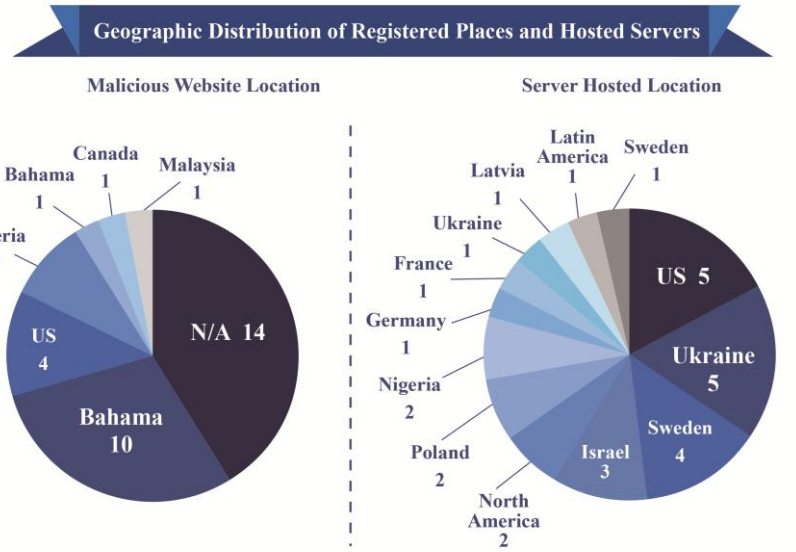
OceanLotus often changes domain names and IP addresses of its download and C2 servers to disguise its true identity. Based on initial statistics, OceanLotus used 35 domain names for the C2 server, with 19 related IP addresses. Most domain names have hidden its Whois information to make it hard for analysts to find the registrants. The picture below shows the registering time and IP information of domain names registered by OceanLotus.



Based on the statistics of related domain names associated with attacks, we sort all domain names by registering time. It turns out OceanLotus registered many new domain names during February and April 2014. Life cycle of the related domain names is as followed.



Registered places and hosted servers are distributed all over the world. As for the registered place, 10 domain names are registered in Bahamas, with 4 in the US and 3 in Nigeria. As for the hosted servers, 5 servers are located in the US and Ukraine each, with 4 in Sweden and 3 in Israel.



Based on registered time, some active domain names are listed below.

Domain Name	IP Binding	Time registered	Target
pad.werzo.net	185.29.8.39	2012/4/17	C2，Mac OS
shop.ownpro.net	185.29.8.39	2012/4/17	C2，Mac OS
ssl.sfashi.com	176.31.22.77	2012/11/7	C2
kiifd.pozon7.net	173.208.157.117	2013/1/8	C2，Mac OS
cdn.libjs.co	62.113.238.135	2013/9/6	C2
sin04s01.listpaz.com	193.169.244.73	2013/11/12	C2
high.expbas.net	91.229.77.179	2014/1/22	C2
img.fanspeed.net		2014/2/8	C2
active.soariz.com	193.169.244.73	2014/2/20	C2
zone.mizove.com	193.169.244.73	2014/2/20	C2
dc.jaomao69.info	146.0.43.107	2014/3/14	Downloader
cdn.jaomao69.info	146.0.43.107	2014/3/14	C2
download.mail-attach.net		2014/4/2	Downloader
cnf.flashads.org	128.127.106.243	2014/4/3	Phishing server
cn.flashads.org	128.127.106.243	2014/4/3	Phishing server，Downloader，DNS
cv.flashads.org	128.127.106.243	2014/4/3	Phishing server
cp.flashads.org	128.127.106.243	2014/4/3	Phishing server
fpdownload.shockwave.flashads.org	128.127.106.243	2014/4/3	Downloader

authen.mail.hairunaw.com.l.main.userapp.org	192.187.120.45	2014/4/8	Downloader
jsquery.net	64.62.174.176	2014/4/8	C2
gs.kroger7.net	167.114.184.117	2014/5/16	C2
autoupdate.adobe.com			Fake Adobe subdomain achieved through domain hijacking for updating malicious program of infected system

OceanLotus Trojan Technologies

From the technical view, OceanLotus used four types of trojans, three of which are for Windows, the other one is for Mac OS. All these four types of trojans and the modules they downloaded have the function of stealing confidential data, but the attack methodology and principle of each have major differences. For the three Windows types, each type becomes more and more complex and dangerous with time. Cloud control techniques are also added in later version. From the evolution of the trojans we are able to see how the technology development roadmap and attack strategy changes.

According to the characteristics of these Trojans, we name the four types of trojans as *OceanLotus Tester*, *OceanLotus Encryptor*, *OceanLotus Cloudrunner*, and *OceanLotus Mac.*

OceanLotus Tester

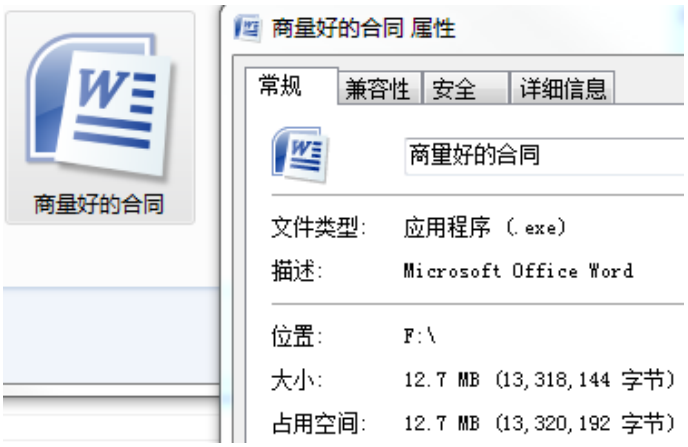
OceanLotus Tester was captured in 2012, which was a simple trojan. The sample was similar to normal spyware and most security software can detect it. From the historical log data, OceanLotus Tester infected a negligible amount of users. After being caught, the sample became inactive for a long period.

However, after correlation analysis of OceanLotus Tester samples with samples from the OceanLotus family, the OceanLotus Tester sample showed significant relationship to OceanLotus, and was considered to belong to the OceanLotus family. The similarities include attack targets, file characteristics, C2 domain names, and pattern of stealing files.

We speculate that OceanLotus Tester may not be an regular tool used by OceanLotus in real attacks. However it is an early stage tool used for testing to determine the feasibility of the system.

OceanLotus Encryptor

OceanLotus Encryptor trojans was first captured in February 2014. At that time, security researchers noticed a set of executables with icon disguised as a Word or JPG document, and with a confusing social engineering file name. The following screen shot is a sample Encryptor trojan disguised as a file named "Discussed Contract" with Word document icon. It is not difficult to figure out that the file is an executable program (.exe).



The major purpose of the Encryptor trojanis to collect, pack and upload Office documents to the C2 servers, including Word, PPT, Outlook mailbox files. Encryptor trojan randomly and recursively encrypts its data sections, increasing the difficulty of being identified by security software.

Once being downloaded and executed, the Encryptor trojan starts a complex process to extract malicious executables. A sample with Word document icon is analyzed as following.

The trojan first extracts a Word document with the same file name of the original executable, and generates a shortcut on the desktop, to confuse the victims. Then the trojan decrypts data in the file and releases a real trojan, with a strong 64-byte key. After starting the real trojan, the original file deletes itself to avoid being detected and captured by security software.

The trojan uses two methods to load a communication module called Bundle.rdb. One is loaded directly and the other is injected into a system process. Once the Bundle.rdb module is loaded, it establishes a connection to the C2 server and sets up the communication channel. The program has also been well-disguised as QQ software (popular instant messaging software in China). The trojan also uses many techniques to try to bypass security software during the loading process. In addition, Encryptor appends garbage data (such as 0x00) to the end of file to avoid being uploaded to cloud-based security platform.

OceanLotusCloudrunner

Cloudrunnertrojan was first captured in November 2014. Compared with the Encryptor trojan, Cloudrunner trojans are small executable files, with no malicious features. After the initial infection, it automatically downloads other modules from specific C2 servers and completes additional tasks. This behavior

is an obviously cloud control feature. Attackers may send different malicious code to the infected computer, according to different purposes. The attack is more subtle and dangerous. The screenshot below shows the properties of such trojan files.

The trojan uses encrypted shellcode, which decrypted and executed in memory, downloading the second stage function modules. The modules collect information and start malicious activities as plugins. By using this mechanism, the footprint of trojan on the user's system is minimized, and functions can be controlled by attackers from the cloud. Known functions utilized by the plugins include:

Functions	**Details**
IM software records	Yahoo、QQ、Skype, etc.
Email data	ThunderBird、Foxmail、Mailease、MS Live、Outlook
File information	Installed software, recent accessed files, device drivers and directories
System information	Account, IP addresses, Shared folders, process list, network connections.
Screenshot	
Network flow	

OceanLotus Mac

OceanLotus Mac was captured at the same time with OceanLotus Encryptor, as the second generation of trojans used by OceanLotus. The trojan targets Mac OS system, used in watering hole attacks. The Apple Mac OS is not a popular APT attack target.

As an example, sample with MD5 9831a7bfcf595351206a2ea5679fa65e is analyzed to demonstrate attack process:

`FlashUpdate.app\Contents\MacOS\EmptyApplication`is a loader to decrypt and release the following files:

```
FlashUpdate.app\Contents\Resources\en.lproj\.en_icon
FlashUpdate.app\Contents\Resources\en.lproj\.DS_Stores
```

`.en_icon` is a copy of the loader, and`.DS_Stores` is the real executable. After released the files, `EmptyApplication` deletes itself.

`.DS_Stores` connects to the following three C2 servers:

- kiifd.pozon7.net
- pad.werzo.net
- shop.ownpro.net

The following remote control commands are implemented:

Function	**Command**
List directory	ls [path]
Change directory	cd [path]
Get working directory	pwd
Delete files	rm<file_path>
Copy files	cp<srcppath><dstpath>
Move files	mv <srcpath><dstpath>
Get process infomation	p {info:pid | ppid | name}
Kill process	kill <pid>
Execute shell command	cmd<command system>
Capture network data	capture <saved_path>
Show file content	cat path [num_byte]
Download file from servers	download fromURLsavePath

- The OceanLotus Mac trojan also has strong self-defense capabilities:

1) Encrypt itself with strong algorithm requires manual decryption to analyze.

2) Modify security settings of Safari browser, to suppress the security prompt when executing downloaded applications

3) Invoke `/bin/launchctl` to regularly execute uploading operations.

4) Detect operating system versions and behave differently. Detect Parallels VM and stop working.

Capability Analysis of OceanLotus

SkyEye Labs has reached a conclusion that there may exist several teams inside OceanLotus through analyzing malicious code, attack payloads and bait data. Each team may collect target social engineering information, develop specific tools and conduct additional data analysis on the stolen information. OceanLotus teams work closely in all aspects together , and they share all the intelligence and payloads internally. In general, in order to achieve the currently known attack effects, Ocean Lotus should have the following capabilities:

1） First, OceanLotus is proficient at the languages of target countries. In addition, they track related current national affairs so they can identify and analyze targeted personnel to attack with specifically designed attacking tools.

2） Secondly, OceanLotus can send spear phishing e-mails, set watering hole traps and extract sensitive data in order to maintain long-term control.

3） Thirdly, OceanLotus is able to develop or obtain particular trojan that can bypass the scan by popular antivirus products.

According to the previous analysis, SkyEye Labs speculate that there may exist three teams inside OceanLotus, and each team has specific capabilities and tasks:

Furthermore, because most of these particular trojans developed by OceanLotus

are named in Chinese and have close links with the latest China political affairs and social concerns. SkyEye Labs believes they have personnel who are well versed in Chinese. They also are acquainted with Chinese national conditions so they can research on specific social engineering effectively.

Capture of OceanLotus Attacks

Increasingly more organizations in China get connected with Internet. The wide application of Internet in the enterprises will bring efficiency as well as network attacks from around the world.

In fact, APT attacks targeting government, organizations and enterprises take place every day. We can even draw the conclusion that APT attack are just around us. OceanLotus is just one typical example of the dozen cases we captured up to now.

At present, many world-renowned security firms have conducted research on APT attacks, and released related reports, such as FireEye, Kaspersky. However, professional study on APT attacks within China is still limited.

One of the reasons of the current situation is the elusive, targeted and confrontational characteristics of APT attacks, which make it hard to detect with normal prevention and trojan removal technologies. The capture and detection of APT attacks has become the focus of security firms and research institutes.

Based on years of experience of Qihoo 360 in Antivirus, vulnerability exploitation & protection, SkyEye Labs makes lots of exploration and practices in detection and removal of sophisticated trojans, 0day/Nday vulnerabilities. The experience and exploration resulted in successful capturing of APT attacks, exploiting sophisticated trojans and vulnerabilities.

In addition to the detection and prevention of sophisticated APT attacks, the capture and research of APT attacks face one greater challenge-----how to correlate network attacks in different time, different places, with different victims and in different forms so as to form a whole picture of the APT attack. Up to now, the research on APT attacks mainly focus on specific and short-term attack processes. Few institutes can conduct long-term and wide reaching APT research.

The APT attacks OceanLotus conducted lasted over 3 years, with over 29 provinces in China and 36 other countries involved. Dozens of websites were hacked for water holing attacks. During the last 3 years, OceanLotus utilized four trojans in different coding patterns and different attacking mechanisms, with malicious servers located in 13 countries and 35 domain names registered.

OceanLotus's APT attacks were long in duration, wide reaching, had a clear purpose and specific targets. It's hard to reconstruct the whole picture of the APT attack campaign using traditional local detection and prevention technologies, though scattered attacks and virus samples might be discovered.

The understanding of OceanLotus and the capture of its APT attacks by SkyEye Labs is mainly owing to the utilization of multi-dimensional data correlation analysis. We make correlative analysis and historic retrieving of billions of malicious programs, billions of protection data of security endpoints, and PB level data from internet and other multi-dimensional data. All kinds of attacking events and elements associated with OceanLotus are finally put together so as to draw a complete picture of the APT attacks targeting China by OceanLotus.

At present, there are few research institutes can discover APT attacks through big data analysis. Meanwhile, few security firms have the capability of big data process and analysis, together with experience in advanced attack and defense. SkyEye Labs based its research on years of accumulated security big data and internet security technologies, thus it can capture threats, hard for other organizations to find, and make correlative analysis of events. We hope our big data based internet security technology can bring help and serve as a reference to other security researchers.

About Qiho 360 & SkyEye Labs

About Qihoo 360

Qihoo 360 Technology Co. Ltd. (NYSE: QIHU) is a leading Internet and mobile platform company in China, measured by user base. By December 2014, Qihoo 360 had about 509 million monthly active Internet users, and over 744 million mobile users.

Recognizing security as a fundamental need of all Internet and mobile users, Qihoo 360 built a large user base by offering comprehensive, effective and user-friendly Internet and mobile security products. Qihoo 360 strives to provide services that protect users' computers and mobile devices against malware and malicious websites.

About SkyEye Labs

Established in Jan. 2014, SkyEye Labs is a specialized team within Qihoo 360 (NYSE:QIHU), focusing on unknown threat research through taking advantages of big data analysis technology. On the strength of Qihoo 360’syears of massive security big data accumulation and data mining technology, SkyEye Labs is capable of identifying, tracing, monitoring and forecasting unknown threats in the entire internet, so as to provide timely and precise threat intelligence for security detection and defense devices.

About 360 SkyEye System

360 SkyEye is a next-generation unknown threat perception system, which can help large organizations like government agencies, financial institutions, energy enterprises and telecom carriers identify and trace unknown threats. By utilizing automatic data mining and cloud-based correlation analysis, 360 SkyEye is able to foresee diverse security threats and deliver customized threat intelligence to clients. Working with on-premise appliances, 360 SkyEye is designed to store and analyze local traffic in depth, to help clients to identify malicious behaviors of unknown threats in their early stage. Furthermore, SkyEye is capable of locating targeted victims and attack sources as well, to trace their intrusion path.


SkyEye
天眼实验室