The Eye of the Tiger

Credits:
Ivan FONTARENSKY  Malware Research
Fabien PERIGAUD  Reverse Engineering
Ronan MOUCHOUX  Threat Intelligence
Cedric PERNET  Threat Intelligence
David BIZEUL  Head of CSIRT
EXECUTIVE SUMMARY

Operation Pitty Tiger – “The Eye of the Tiger”

Cyber espionage has been a hot topic through the last years. Computer attacks known as “APT” (Advanced Persistent Threat) have become widely reported and emphasized by the media, damages are now considered as real and strategic trends are moving in cyber defense.

AIRBUS Defence & Space – CyberSecurity unit responds to such attacks for its customers every day, developing a complete range of solutions.

Today, we decided to release publicly information on a specific group of APT attackers known as “Pitty Tiger”. This information comes directly from investigations led by our Threat Intelligence.

Pitty Tiger is a group of attackers that have been active since at least 2011. They have targeted private companies in several sectors, such as defense and telecommunications, but also at least one government.

We have been able to track down this group of attackers and can provide detailed information about them. We were able to collect and reveal their “malware arsenal”. We also analyzed their technical organization.

Our investigations indicate that Pitty Tiger has not used any 0day vulnerability so far, rather they prefer using custom malware, developed for the group’s exclusive usage. Our discoveries indicate that Pitty Tiger is a group of attackers with the ability to stay under the radar, yet still not as mature as other groups of attackers we monitor.

Pitty Tiger is probably not a state-sponsored group of attackers. They lack the experience and financial support that one would expect from state-sponsored attackers. We suppose this group is opportunistic and sells its services to probable competitors of their targets in the private sector.

We have been able to leverage several attackers profiles, showing that the Pitty Tiger group is fairly small compared to other APT groups, which is probably why we saw them work on a very limited amount of targets.

At the end of this report, we provide indicators of compromise to help people detect current Pitty Tiger attacks.
# TABLE OF CONTENT

**EXECUTIVE SUMMARY** ........................................................................................................ 2  
**TABLE OF CONTENT** ........................................................................................................... 3  
**MODUS OPERANDI: APT ATTACKS** .................................................................................. 5  
  - Reconnaissance phase ........................................................................................................... 5  
  - Initial compromise ............................................................................................................... 6  
  - Access strengthening & lateral moves ............................................................................. 6  
  - Data exfiltration ................................................................................................................. 7  
**“PITTY TIGER” INVESTIGATION CONTEXT** .................................................................... 8  
**INFECTION METHODS** ....................................................................................................... 9  
  - Spear Phishing and weaponized documents ................................................................... 9  
  - Direct attacks .................................................................................................................... 10  
**MALWARE INFORMATION** ................................................................................................ 12  
  - Troj/ReRol.A ..................................................................................................................... 12  
  - PittyTiger RAT .................................................................................................................. 16  
  - CT RAT ............................................................................................................................. 19  
  - MM RAT (aka Troj/Goldsun-B) ....................................................................................... 23  
  - Paladin RAT ....................................................................................................................... 26  
  - Leo RAT .............................................................................................................................. 28  
**INFRASTRUCTURE** ............................................................................................................ 30  
  - Avstore.com.tw .................................................................................................................. 30  
  - Skypetm.com.tw ................................................................................................................ 32  
  - Common characteristics between the two domains ......................................................... 35  
  - Other domains linked with the Pitty Tiger group ............................................................. 36  
**VICTIMS** ............................................................................................................................. 39  
**ATTACKERS** ......................................................................................................................... 40  
  - Attacker’s connections to the c&c .................................................................................... 40  
  - “TooT” ............................................................................................................................... 44  
  - “Cold & Snow” ................................................................................................................... 48  
  - Roles and organization ...................................................................................................... 48  
  - Attackers arsenal ............................................................................................................... 49  
**ATTRIBUTION** ......................................................................................................................... 53  
**CONCLUSION** ......................................................................................................................... 56  
**INDICATORS** .......................................................................................................................... 57  
  - Domains ............................................................................................................................ 57  
  - Malware hashes ............................................................................................................... 57  
  - Malware Strings ................................................................................................................. 58
MODUS OPERANDI: APT ATTACKS

APT attacks follow what we call the “APT kill chain”. The kill chain describes briefly the way attackers do perform their actions.

It can be summarized by the following scheme:

**RECONNAISSANCE PHASE**

The reconnaissance phase commences when an attacker selects a new target and involves the acquisition of information about that target.

There is very little information available about this phase, and there is little data about it. The only way to collect information about this phase would be to already monitor all attackers’ actions at this step, which is hardly feasible.

The longer the attackers spend time in attempting to understand their target and its online presence, the easier it will be to find efficient ways to penetrate that company’s systems.

This reconnaissance phase is both about finding information to break into the targeted network successfully and about searching for data which could help to accelerate sensitive information isolation (like the name of a key employee for example).
This phase mostly relies on open sources from the Internet: social networks, press releases, white papers, corporate websites, search engines, but also on some active tools like vulnerability scanners etc.

INITIAL COMPROMISE

At this stage, the APT attackers have a solid knowledge of their target and its key employees. The attackers have everything they need to start looking for an entry point to the company’s network and establish one or several permanent backdoors into the environment.

The attackers mostly rely on two techniques here to infect one or several computers, usually workstations, inside the target’s network: spear phishing and drive-by downloads.

Spear phishing can be described as targeted e-mail phishing. In a spear phishing scheme, attackers send very few e-mails to targeted people. In fact, they can even send just a single e-mail. The trick is to target the right victim and provide it with the right content, so that they will click on a link leading to drive-by download of a malware, or open an attached file which will infect their computer.

Some groups of attackers also use “watering hole” techniques to successfully compromise their targets. To build a watering hole attack, attackers do compromise the website of a third party, generally a supplier of the target, which is typically visited by a specific group of professionals and very likely by the target. Every visitor of the compromised third party is then infected. The method has one major drawback: it will also infect third parties who visit the website. Attackers have developed ways to avoid this. If their reconnaissance phase has been done effectively, they already know all IP ranges used by the target company. It just takes a few lines of code in the infecting script to only compromise visitors coming from the target IP ranges.

Direct attacks against servers of the target can also be a way to penetrate the target’s network.

ACCESS STRENGTHENING & LATERAL MOVES

Attackers have gained access to one or several machines inside the target’s corporate network. They need to install several different backdoors in order to be able to always access the network. In case one backdoor falls, there will be others.

As soon as the attackers are sure they have enough access, they start looking for two things: intellectual property (or anything else they want to know or steal) in alignment with predefined mission objectives, and a means of privilege escalation to facilitate lateral movement within the compromised environment. It generally does not take long before the attackers gain domain administrator privileges and dump all the Active Directory content.

They use lateral moves between machines inside the network, and look for everything they need. This step is very hard to detect, since they only use valid credentials and legitimate administration tools such as PsExec.
DATA EXFILTRATION

Data exfiltration is the last step before the attackers loop to the lateral moves step, in a never-ending circle of prolonged access and information theft.

They generally create archive files containing the content they want to exfiltrate, which are then sent to the attackers by using a remote administration tool (RAT) or transfer protocols such as FTP and HTTP.

This phase is not the end of an APT attack. The attackers loop to the access strengthening/lateral moves stage and generally keep stealing more information and stay inside the network for more data gathering.

For more information about all the APT phases, please refer to our APT Kill Chain blog post serie¹.

¹ http://blog.cassidiancybersecurity.com/tag/APT
“PITTY TIGER” INVESTIGATION CONTEXT

During our regular investigations on APT cases, one particular variant of malware caught our attention, because we had not faced it before. We decided to spend some time to investigate around this malware and found out that it was used exclusively by a single group of attackers. This malware family is known as “PittyTiger” by the anti-virus research community.

We discovered this malware sample in June 2014, leading to a command & control (c&c) server still in activity.

Our researches around this particular malware family revealed the “Pitty Tiger” group has been active since 2011, yet we found other publications1 which could probably be attributed to the same group of attacker back in 20102.

This group uses other malware and tools during their APT operations, in addition to the PittyTiger RAT.

A variant of the infamous Gh0st RAT dubbed “Paladin” has been used repeatedly by the PT group, together with other RATs which seem to be developed exclusively for the PT group: “MM RAT” (aka Troj/Goldsun-B), and “CT RAT”. Another variant of Gh0st RAT named “Leo” has been found inactive on a c&c server.

We also found another malware, named “Troj/ReRol.A”. This one is also used by the group to infect workstations, collect system information, and install more malware on the infected computer. It acts as a first stage downloader and system data collector often used in the initial compromise of the Pitty Tiger campaigns, generally embedded in Microsoft Office documents.

Thanks to server's misconfigurations, we managed to get information from three c&c servers used by this group of attackers, which provided us with insight from the end of 2013 to the beginning of July 2014.

Our investigation has been focused on the data we could get from these c&c servers but also on the Pitty Tiger environment.

This whitepaper aims to expose the view we have on the group, especially on their infrastructure and capabilities. We hope this publication will bring further counter analysis from the research community to enrich the global common threat knowledge.

1 http://nakedsecurity.sophos.com/2012/08/03/poisoned-doc-targeted-malware-attack/
2 http://nakedsecurity.sophos.com/2010/06/24/targeted-trident-cyberattack-defence-company/
INFECTION METHODS

SPEAR PHISHING AND WEAPONIZED DOCUMENTS

Pitty Tiger, like most other APT groups, use spear phishing e-mails extensively in order to gain an initial foothold within the targeted environment.

We have been able to find a spear phishing e-mail crafted by the attackers. This e-mail spoofed the identity of an employee of a targeted company:

From: XXXXXXX
To: XXXXXXX
File: 1 Attachment: Bird’s Eye Point of View.doc

While the holiday season means clustering, clustering ‘time for a vacation’ for many, there are Those That Will Be of us staying home this year. That’s why we’ve Decided to take you on a trip around the world from a bird’s eye view of the item! It’s safe to say That MOST of the lucky people on vacation Will not see breathtaking sights like these. Remember to look down!

The attached file is a Microsoft Office Word document triggering CVE-2014-1761 to infect the computer it is sent to:

Word document used to infect computers with Troj/ReRol.A
While this example looks very “amateur” for a spear phishing attempt, we suppose the group has conducted more advanced spear phishing campaigns, based on the fact that we found infected Word documents showing content stolen from victims of the group. These documents were infecting the system with Troj/ReRol.A malware, which we will detail later in this report.

This could mean that the Pitty Tiger group is using stolen material as spear phishing content either to target other persons in the compromised company, or to target other persons in a competitor's company, or more generally to compromise another target.

Pitty Tiger also seem to use fake Microsoft Office Excel content, yet we could only find empty content delivering once again the Troj/ReRol.A malware.

**DIRECT ATTACKS**

Although we have not been able to find evidences of any attack aimed at exploiting vulnerabilities on the group’s targets servers, we have been able to record several vulnerability scanning launched from one c&c server straight to the targets.

The attackers have been using different vulnerability scanners aimed at their targets. While some targets have been scanned with "generic" vulnerability scanning tools like HScan or Fluxay and port scanners like Nmap, some other targets have been scanned for very specific vulnerabilities, like a ZyWALL vulnerability or a FORTINET product.

We have also been able to testify that the Pitty Tiger group has successfully collected information on some of their targets by exploiting the HeartBleed1 bug. This vulnerability which exists on some old versions of OpenSSL allows attackers to collect data from chunks of memory from the targeted machine. It allowed the Pitty Tiger group to get admin credentials from at least one target, for example.

![Memory data leak from one server – Heartbleed exploit on one of PittyTiger's targets](image)

---

Running automated vulnerability scanners on whole ranges of IP addresses used by the targets or on several domains is a very noisy way to collect information and find server vulnerabilities. We would advocate that this method is unwise when you want to stay furtive, and doing it from a c&c server is very surprising, to say the least. While the Pitty Tiger group is experienced on some aspects on its running APT campaigns, it definitely lacks some maturity here.
MALWARE INFORMATION

**TROJ/ReRol.A**

One of the favorite methods used by the Pitty Tiger group to infect users is to use a Microsoft Office Word document which exploits a specific vulnerability.

The payload infecting the system is malware known as “TROJ/ReRol.A”. It is generally the first step of the initial compromise for Pitty Tiger campaigns.

**Exploitation**

We have been able to find one such document\(^1\) used by that group of attacker, exploiting CVE-2012-0158, an old critical vulnerability impacting Microsoft Office and corrected by Microsoft's MS12-027 fix in April 2012. This vulnerability affects Microsoft Office versions up to Office 2010. We also found one RTF document embedding CVE-2014-1761, which is a more recent exploit.

We discovered several different documents spreading this malware by triggering CVE-2012-0158 vulnerability, yet we could not share them in this report, since these documents contain information about victims of the Pitty Tiger group.

The discovery of this “old” vulnerability exploitation in June 2014 could mean that the Pitty Tiger group has no direct access to 0day exploits, or not enough budgets to buy some. It could also mean they use their low range exploit by default because it is working on their targets and is sufficient to compromise their workstations.

The Word document we initially found was probably a “test” document used by the group. When opened, it shows a single line written in Chinese language, which can be translated as “Hello!”

![Microsoft Office Word decoy “test document” used by the Pitty Tiger group](image)

**Installation**

When successfully triggered, the exploit infects the host by dropping and executing a file named “svohost.exe”\(^2\) in the temporary folder of the currently logged-in user:

\(^1\)MD5 hash: e70c0479c9db9a031a263740365e7939
\(^2\) MD5 hash: 1752aacc08ee0acd58405e9bc10b0dbb
This binary is “Troj/ReRol.A” according to Sophos naming convention. It immediately triggers alarms on our sandbox:

![Image of Risk Assessment with 100% risk level]

**Alarms in our sandbox system, triggered by the Troj/ReRol.A malware**

The binary drops a copy of itself in the Application Data folder of the currently logged-in user:

![Image of File Activity showing C:\DOCUME~1\USER\LOCALS~1\Temp\svohost.exe]

**Creation of a copy of the Pitty Tiger malware in a user folder in our sandbox**

The malware initiates a communication to time.windows.com to check for connectivity, and then communicates with the c&c server at `mac.avstore.com.tw`.

---

Very few variants of Troj/ReRol.A are public. The variants we have seen did use that same User-Agent:

**Mozilla/4.0 (compatible;**

The persistence mechanism used by the malware is the creation of a registry key named “Shell” containing the path to the malware on the infected system:

```
Key Path: \REGISTRY\USER\<SID\\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
Value Name: Shell
Value: explorer.exe,C:\DOCUME~1\XXXXXX\APPLIC~1\svohost.exe,
```

The payload of this malware is used to collect information on the newly infected host, and send it back to the c&c server. It can also download and execute binaries.

**Command & Control**

The data sent in the POST request has a 0x11 bytes header consisting of a fixed-value byte (0xc3) followed by a 0x10 bytes encryption key. The data following the header is encrypted using RC4 with the previous key. Once the data is deciphered, the last byte of the clear text should also be 0xc3.

We have been able to decrypt the communications and confirmed what is transmitted to the c&c server.
Here is an anonymized sample of communication showing information collected by the malware:

```
HostName :xxx
UserName :xxx
SysType  :32bit

Windows 7 Enterprise Service Pack 1 6.1 7601
Organization: Owner:xxx

---------------------Server Info---------------------
- AdobeARMservice
- Adobe Acrobat Update Service
- AeLookupSvc
- Application Experience
- AudioEndpointBuilder
- ... (list goes on)

---------------------Soft Info---------------------
1   Adobe AIR 4.0.0.1390
2   Adobe Shockwave Player 12.0 12.0.9.149
3   FileZilla Client 3.7.4.1 3.7.4.1
4   Mozilla Thunderbird 24.3.0 (x86 en-US) 24.3.0
5   ... (list goes on)

---------------------IP Config---------------------
Adapt Type: Ethernet
NetCardNum: 11
NetCard Name: {XXX-XXXX-XXXX-XXXX-XXXXXXX}
Description : Realtek RTL8139C+ Fast Ethernet NIC
MAC ADDR: XX-XX-XX-XX-XX-XX
IP Addr: 10.xxx.xxx.xxx
IP Mask: 255.255.255.0
GateWay: 10.xxx.xxx.xxx
DHCP Serv: 1
DHCP Host: 10.xxx.xxx.xxx
WINS Serv: 0
WINS PriHost: WINS SecHost:
```

Sample information collected by Troj/ReRol.A malware

This information is very useful for an attacker: it shows all software installed on the system, and running services.

Once this data has been transferred to the c&c server, it responds by sending additional malware to execute on the machine.

The c&c part consists of two files:
- **dr.asp**: an ASP frontend instantiating a control, setting some variables, and passing the payload.
- **JHttpSrv.dll**: a controller which should be registered via “regsvr32”. It exposes 4 methods which can be called by the ASP script:
  - **SetIP(strIP)**: sets the bot IP address
  - **AddKeyword(strKeyword, strFilePath)**: binds a keyword to a binary on the server
  - **Work(lpByteArray, nDataLength)**: deciphers the payload, looks for the registered keywords, and writes it to a logfile
  - **ResponseBinary()**: sends back the binary matching a specific a keyword
The dr.asp registers the following keywords:
- “SysType :32bit” to the binary “32.exe”
- “SysType :64bit” to the binary “64.exe”

These two binaries were no longer available on the server. However, we found various files which could have been used as “32.exe” in the past:
- 3200.exe
- 322.exe
- 32m.exe
- 32mm.exe

The 322.exe file is a legitimate, Chinese, calc.exe tool. It might have been used by the attackers to perform tests.

The 3 others binaries are RATs, which will be detailed in the next parts.

**PittyTiger RAT**

This RAT is the origin of the attackers’ group name. “PittyTiger” is a mutex used by the malware. “Pitty Tiger” is also a string transmitted in the network communications of the RAT, as you will see in this chapter.

**Installation**

The malware\(^1\), when running in our sandbox, triggers the following alarms:

### Risk Assessment

| Alarms in our sandbox system, triggered by the PittyTiger malware |
|---------------------|---------------------|
| **PROCESSORS ACTIVITY** | **FILES ACTIVITY** | **RESISTANCE** | **NETWORK ACTIVITY** | **SYSTEM ALTERATION** |
| Severe | 100% | 80% | 100% | 80% | 20% |

The binary drops two files in “C:\Windows\System32”:

\(^1\) MD5 hash: be18418cafdb9f86303f7e419a389cc9
Files dropped by the PittyTiger RAT in our sandbox

The “qmgrxp.exe” binary is a simple copy of the original binary. It drops the “packet64.dll”, and injects it in “explorer.exe”. When executed, a mutex called “PittyTiger” is created.

Persistence is achieved by adding the path to the binary to the WinlogonUserInit key:

Key Path: \REGISTRY\USER\<SID>\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
Value Name: UserInit
Value: C:\WINDOWS\system32\userinit.exe,C:\WINDOWS\system32\qmgrxp.exe,

The “packet64.dll” is the main payload of the RAT. After being injected, it starts sending its Hello packet to its c&c server:
Command & Control

All the requests sent to the c&c contains the string “/FC001/” followed by the bot id. This id consists of the infected computer name followed by a dash and the lower word of the disk serial id.

The data sent is simply encoded using base64, there is no cipher at all. The hello packet, once decoded, looks like the following:

```
--------------------------PittyTigerV1.0--------------------------
--------------------------
--------------------------^ ^--------------------------
--------------------------^--------------------------
Version:NULL
```

Our sample had 3 c&c servers configured:
- jackyandy.avstore.com.tw:80
- chanxe.avstore.com.tw:443
- newb02.skypetm.com.tw:80

The following commands are implemented:
- File Download (get) and Upload (put)
- Screen Capture 8bit (prts) and 16bit (prts2)
- Remote Shell (ocmd/ccmd)
- Configuration update (setserv/freshserv)
- Direct command execution

Regarding the controller part, we found two different versions:
- A Delphi binary handling PittyTiger connections only
- A .NET binary handling both PittyTiger and CT connections

The interface handling both Pitty TIGER and CT connections is very interesting. We have been able to confirm that the author of those two families of malware is the same person, as will be seen in the next chapter about “CT RAT”.

---

Pitty Tiger RAT – controller part
CT RAT

This remote administration tool is often used by the Pitty Tiger group. We have been able to acquire both the client and the server parts.

We found two instances of the same binary with different names – 32mm.exe and mm32.exe.

This RAT seems to be an evolution of PittyTiger, since a specific server binary we found could handle both requests from CT and PittyTiger, and was indicated as compatible with PittyTiger. Moreover, the same commands are implemented in both RATs.

Installation

Unsurprisingly, when running in our sandbox, the RAT triggers the same alarms as PittyTiger:

![Risk Assessment Chart](image)

Alarms in our sandbox system, triggered by the CT RAT

The binary drops two files in “C:\Program Files\Internet Explorer”:

1 MD5 hash: f65dc0b3eeb3c393e89ab49a3fac95a8
The “ieupdate.exe” is a simple binary to inject the DLL into “explorer.exe”. Persistence is achieved via the following registry key:

**Key Path:** \REGISTRY\USER\<SID>\Software\Microsoft\Windows NT\CurrentVersion\Windows

**Value Name:** load

**Value:** c:\PROGRA~1\INTERN~1\ieupdate.exe

After injection, the RAT sends a first login packet to its c&c:

Encrypted communication from a machine infected with CT RAT

**Command & Control**

The RAT communication is performed through HTTP requests. The data is sent encrypted with RC4, and base64-encoded. The RC4 key is the Unicode form of the requested URL.
The Login packet contains the following string, after decoding and deciphering:

```
Login
->C:PC-XXX
->U:User-XXX
->L:10.10.10.1
->S:Microsoft Windows XP Service Pack 3 5.1 2600
->M:Nov 13 2013
->P:1033
```

It contains the computer name, the user name, the internal IP address, the OS version, the RAT internal version and the Language ID of the system.

The RAT can then receive commands from its c&c. Usual RAT features are implemented:
- File Download (GET) and Upload (PUT)
- Remote shell (ocmd/ccmd)
- Configuration update (cfg)
- Sleep (sleep)

**Version and author(s)**

Regarding the configuration, our sample communicates with "sop.avstore.com.tw", and contains the string "Nov 13 2013", which should be a version identifier.

The c&c part is a Windows binary written in .NET. We found 2 versions:
- Version 2013.10: CT only controller
- Version 2013.12: CT and PittyTiger controller

The About form gives the name of the developer(s):
The version of the controller which can handle both PittyTiger and CT shows the same author(s):
As these screenshots show, the switch between PittyTiger and CT was probably in the last semester of 2013.

The text can be translated, thanks to Google Translate, as:

CT console (compatible pittytiger) v1.3
2013.12 by Trees and snow

Further discussion about this author is provided in subsequent sections.

**MM RAT (aka troj/goldsun-b)**

We named this malware “MM RAT” at the beginning of our investigation, before we found an existing name for it, “Troj/Goldsun-B” according to Sophos. This is another remote administration tool often used by the Pitty Tiger crew. We have been able to acquire both a client and server part for it.

**Installation**

The binary we found is named 3200.exe¹, and triggers the following alarms in our sandbox:

![Risk Assessment Diagram]

The “release.tmp” file is dropped on the system:

---

¹ MD5 hash: 728d6d3c98b17de3261eaf76b9c3eb7a
The binary is also copied to the user’s “Application Data” directory, and injects the “release.tmp” file in “explorer.exe”.

Persistence is achieved by adding the path to the binary to the Winlogon Shell key:

```
Key Path: \REGISTRY\USER\<SID>\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
Value Name: Shell
Value: explorer.exe,C:\DOCUME~1\<UserName>\APPLIC~1\<binary name>,
```

The RAT embeds its own DNS server IP addresses to make the c&c domain names resolutions. These addresses are listed below:

- 63.251.83.36
- 64.74.96.242
- 69.251.142.1
- 212.118.243.118
- 216.52.184.230
- 61.145.112.78
- 218.16.121.32

**Command & Control**

It starts resolving its domains after injection, and immediately sends requests. First requests are used to check for updates (GET request on /httpdocs/update/update.ini). A Hello packet is then sent:
The bot then repeatedly sends GET requests on “/httpdocs/mm/<bot_id>/ComMand.sec” to retrieve remote commands. The communication protocol is quite simple: GET requests are used to receive data from the c&c, and POST requests to send data. In POST commands, the CGI name represents the command.

The following features are implemented:
- c&c authentication using password
- Remote shell
- Remote commands
- File Download / Upload / Deletion / Search
- Bot termination

The following CGI files can be requested by the bot:
- Vip: test for connectivity
- Owpp4: register new bot
- CReply: answer to remote commands
- Clrf: clear remote file (to clear ComMand.sec after reading)
- CFile: transmit file (file transfers or answers to commands)
- Cerr: send error

The configuration is stored locally in a file called “schmup.sys”. The file is ciphered using RC4, using the MD5 hash of “rEdstArs” as the key.

Our sample uses “mca.avstore.com.tw”, “star.yamn.net” and “bz.kimoo.com.tw” as c&c servers. It contains the “1.6.0” version number, and uses the password “9ol.8ik,” to authenticate with the bots.

Unlike others c&c binaries, the c&c part of this RAT does not have a graphical interface, but can be remotely requested to manage the bots. Furthermore, no authentication is required to send commands to the c&c (but you need to know the configured password to interact with the bots).

The management protocol is the same as the bots protocol, with different CGI files:
- Shutdown: shutdown the c&c
- Cnor: add a new command for a bot (writes it in “ComMand.sec”)
- Mlist: get the list of bots
- Mlist2: write the list of bots to the file “Online.dat”
The bots’ answers to remote commands can be retrieved by requesting the “Reply.sec” file (e.g. GET /httpdocs/mm/<bot_id>/Reply.sec)

**Network patterns**

These network patterns might ring bells in some researcher’s minds. The network communication used by this binary are the same as those used by the Enfal malware, which has been used in the past by the Lurid group (APT attackers) and by other threat actors in China¹.

An examination of the code did not reveal code similarities with the Enfal malware. We do not currently know why this malware uses the same patterns to communicate.

**PALADIN RAT**

This is another remote administration tool used by the Pitty Tiger group. We have been able to get both a client and server part of it.

**Installation**

The binary we found was dropped by a malicious Word document. The following alarms are triggered in the sandbox:

![Risk Assessment Chart](image)

The shellcode contained in the Word file drops the following file, and executes it:
- C:\Documents and Settings\<User>\Local Settings\Temp\svohost.exe²

This one drops in turn the following file:

---

² MD5 hash: 0567fd7484efbae502cac279d32ed518
This tmp file is then copied to “C:\Windows\system32\Nwsapagentex.dll” and registered as a service called “Nwsapagent”.

This malware is a variant of the infamous Gh0st RAT\(^1\). Our specific sample uses “ssss0” instead of the usual “Gh0st” header for network communications.

**Command & Control**

The commands ID used in the communication protocol have also changed, but the features are quite the same.

The configuration is directly embedded in the binary, and deciphered at runtime. Up to 5 c&c servers can be configured, but our sample only had one: “ey.avstore.com.tw:53”.

“EY” could stand for “Ernst & Young”. It would not be very surprising, since a lot of different attack groups do use anti-virus vendors or other big company’s names to try to look more legitimate. Pitty Tiger is no exception, as detailed later in this report.

We also found two c&c binaries, claiming to be versions 2.1 and 2.2 of the Paladin RAT controller. Version 2.1 answers to the “ssss0” header, while version 2.2 uses the classical “Gh0st” header.

\(^1\)http://www.mcafee.com/sg/resources/white-papers/foundstone/wp-know-your-digital-enemy.pdf
Paladin has multiple features: file transfer, screenshot, command shell …

**Leo RAT**

Additionally to the Paladin RAT, we found another variant of Gh0st RAT, named “Leo”. Although we have found it on a c&c server of the group, there is no evidence that it has been used by the group, in opposition to Paladin which is used often by Pitty Tiger.

Moreover, the built malware we found in the same folder was configured to connect to a local IP address, probably for testing purposes.
Leo malware controller screenshot – a variant of Gh0st RAT
INFRASTRUCTURE

Our investigation has focused on three particular c&c servers used by the group. These c&c servers, unlike the other c&cs used by the group, have been misconfigured. Once parsed and dumped, it provided us with more insight.

We found several domains used by the Pitty Tiger group, the most interesting ones being detailed in this chapter.

Pitty Tiger, like other APT attackers, often use anti-virus “familiar names” when registering domains or creating subdomains. Some examples can be avstore.com.tw, sophos.skypetm.com.tw, symantecs.com.tw, trendmicro.org.tw etc.

AVSTORE.COM.TW

WHOIS Data

The registration information for this domain has been the same since 2013-06-04:

Domain Name: avstore.com.tw
Registrar: information of network company
longsa longsa33@yahoo.com
+86.88885918
No.520.spring road.shenyang
shanghai, shanghai
CN

This information has been used to register another domain, skypetm.com.tw, which has also been used by the Pitty Tiger group.

Malware families

Our research also led us to the discovery of four different malware families connected to subdomains of avstore.com.tw:

- PittyTiger RAT (aka Backdoor:Win32/Ptiger.A)
- Troj/ReRol.A
- CT RAT
- Paladin RAT (variant of Gh0st RAT)
Operation Pitty Tiger – “The Eye of the Tiger”

<table>
<thead>
<tr>
<th>MD5 hashes of files linked to avstore.com.tw</th>
<th>Paladin dropper</th>
<th>eye.avstore.com.tw</th>
</tr>
</thead>
<tbody>
<tr>
<td>0d3b3b422044759b4a08a7ad8afe55c7</td>
<td>Exploit:Win32/CVE-2012-2539</td>
<td>mac.avstore.com.tw</td>
</tr>
<tr>
<td>75cf4f853f0f0350fac9be87371f15c8d</td>
<td>Troj/ReRol.A dropper</td>
<td>sop.avstore.com.tw</td>
</tr>
<tr>
<td>b6380439f9ed006d645759da0f3b05b8</td>
<td>CT RAT</td>
<td>chanxe.avstore.com.tw</td>
</tr>
<tr>
<td>5e2360a8c4a0ce1ae22919d8bf49f0d</td>
<td>PALADIN</td>
<td>jackyandy.avstore.com.tw</td>
</tr>
<tr>
<td>f65dc0b3eeb3c393e89ab49a3fac95a8</td>
<td>Pitty Tiger RAT</td>
<td>jackyandy.avstore.com.tw</td>
</tr>
</tbody>
</table>

Links between malware samples, malware families, and avstore.com.tw subdomains
## C&C servers and IP addresses

<table>
<thead>
<tr>
<th>Hosting company</th>
<th>Geolocation</th>
<th>IP Range</th>
<th>IP Address</th>
<th>Host</th>
<th>Time space</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hongkong Dingfengxinhui Bgp Datacenter</td>
<td>Kowloon, Hong Kong</td>
<td>122.10.0.0 – 122.10.63.255</td>
<td>122.10.48.189</td>
<td>chanxe.avstore.com.tw, jackyandy.avstore.com.tw</td>
<td>Actually in use</td>
</tr>
<tr>
<td>Hurricane Electric Inc</td>
<td>Fremont, USA</td>
<td>66.220.0.0 – 66.220.31.255</td>
<td>66.220.4.100</td>
<td>mac.avstore.com.tw, sop.avstore.com.tw, ey.avstore.com.tw</td>
<td>Actually in use</td>
</tr>
<tr>
<td>New World Telephone LTD</td>
<td>Hong Kong City, Hong Kong</td>
<td>58.64.175.0 – 58.64.175.255</td>
<td>58.64.175.191</td>
<td>jackyandy.avstore.com.tw</td>
<td>Dec. 2013</td>
</tr>
</tbody>
</table>

**SKYPETM.COM.TW**

**WHOIS Data**
This domain has shown two different WHOIS entries through time:
- From 2011-12-29 to 2013-01-02:

Registrant: chenzhizhong  
Email: hurricane_huang@163.com  
Telephone: +86.2426836910

- From 2013-11-21 until today:

Registrant: long sa  
Email: longsa33@yahoo.com  
Telephone: +86.88885918

The most recent registration information is also used for avstore.com.tw.

**Malware families**

Six malware families have been identified as communicating with subdomains of skypetm.com.tw:

- MM RAT
- Pitty Tiger RAT
- Troj/ReRol.A
- CT RAT
- Paladin
- Exadog

<table>
<thead>
<tr>
<th>MD5</th>
<th>Malware family</th>
<th>C&amp;C server</th>
</tr>
</thead>
<tbody>
<tr>
<td>81fa811f56247c236566d430a4798eb</td>
<td>MM RAT</td>
<td>ms11.skypetm.com.tw</td>
</tr>
<tr>
<td>55e456339936a56e73a7883ea1ddb672</td>
<td>Backdoor:Win32/Ptiger.A</td>
<td>botemail.skypetm.com.tw</td>
</tr>
<tr>
<td>d5da60d678d5a55a847e16723c7a4d0</td>
<td>Backdoor:Win32/Ptiger.A</td>
<td>aniu.skypetm.com.tw</td>
</tr>
<tr>
<td>0750569cf1733d4fbb01169476387cc2</td>
<td>Backdoor:Win32/Ptiger.A</td>
<td>aniu.skypetm.com.tw</td>
</tr>
<tr>
<td>abb0abf252e4bf9106273df3c1c2</td>
<td>Backdoor:Win32/Ptiger.A</td>
<td>aniu.skypetm.com.tw</td>
</tr>
<tr>
<td>c0656b66b9f180e59e1fd2f91a85f2</td>
<td>Troj/Rerol.A</td>
<td>zeng.skypetm.com.tw</td>
</tr>
<tr>
<td>ce15fa3338b7fe8e05c511d5e49a98</td>
<td>Troj/Rerol.A</td>
<td>zeng.skypetm.com.tw</td>
</tr>
<tr>
<td>8a54ab33761d1c03605665ca55be7400</td>
<td>Backdoor:Win32/Ptiger.A</td>
<td>qinoo.skypetm.com.tw</td>
</tr>
<tr>
<td>a1ea6dc12b983c726fe76c1b3663b24</td>
<td>Backdoor:Win32/Ptiger.A</td>
<td>qinoo.skypetm.com.tw</td>
</tr>
<tr>
<td>b6380439ff9ed0c6d45759da0f3b05b8</td>
<td>Troj/Rerol.A dropper</td>
<td>sophos.skypetm.com.tw</td>
</tr>
<tr>
<td>5e2360a8c4a0ce1ee22919d8bf49fd</td>
<td>Troj/ReRol.A</td>
<td>sophos.skypetm.com.tw</td>
</tr>
<tr>
<td>79e48961d1ee982a466d22671a42cc</td>
<td>Troj/ReRol.A</td>
<td>sophos.skypetm.com.tw</td>
</tr>
<tr>
<td>0a204387f7a02c115deea2110f961fd3</td>
<td>ReRol.A</td>
<td>sophos.skypetm.com.tw</td>
</tr>
<tr>
<td>b9f5e89906b8a17fd611002660fff32</td>
<td>ReRol.A</td>
<td>sophos.skypetm.com.tw</td>
</tr>
<tr>
<td>4ce8593c9de2b27b5c389f651c81638b</td>
<td>CT RAT</td>
<td>newb02.skypetm.com.tw</td>
</tr>
<tr>
<td>8df89df484ca5c376b763479e0a08d036</td>
<td>Paladin</td>
<td>newb02.skypetm.com.tw</td>
</tr>
<tr>
<td>22e47c5e3809a4150d0db7f99a68cc0</td>
<td>Office Excel file – ReRol.A dropper</td>
<td>margo.skypetm.com.tw</td>
</tr>
<tr>
<td>dd87c68c1e71b104a48a66e87a2349f</td>
<td>Backdoor:Win32/Ptiger.A</td>
<td>ripper.skypetm.com.tw</td>
</tr>
<tr>
<td>068870c2c165a1d29fc2f3d3edfed3ae</td>
<td>Win32/Exadog.AA</td>
<td>link.skypetm.com.tw</td>
</tr>
<tr>
<td>Unknown</td>
<td>Backdoor:Win32/Ptiger.A</td>
<td>asdf.skypetm.com.tw</td>
</tr>
</tbody>
</table>
### Skype.com.tw Infrastructure: Subdomains and Malware Linked to It

<table>
<thead>
<tr>
<th>Hosting Company</th>
<th>Geolocation</th>
<th>IP Range</th>
<th>IP Address</th>
<th>C&amp;C server</th>
<th>Timeline</th>
</tr>
</thead>
<tbody>
<tr>
<td>Take 2 Hosting Inc.</td>
<td>San Jose, USA</td>
<td>173.252.192.0 - 173.252.255.255</td>
<td>173.252.198.103</td>
<td>newb02.skype.com.tw</td>
<td>Actually in use</td>
</tr>
<tr>
<td>Hurricane Electric Inc.</td>
<td>Fremont USA</td>
<td>66.220.0.0 - 66.220.31.255</td>
<td>66.220.4.100</td>
<td>sophos.skype.com.tw</td>
<td>Actually in use</td>
</tr>
<tr>
<td>Taiwan Academic Network</td>
<td>Taipei, Taiwan</td>
<td>210.60.0.0 - 210.60.255.255</td>
<td>210.60.141.45</td>
<td>botemail.skype.com.tw</td>
<td>2012-03-06</td>
</tr>
<tr>
<td>Gorillaservers Inc.</td>
<td>Los Angeles, USA</td>
<td>198.100.96.0 - 198.100.127.255</td>
<td>198.100.121.15</td>
<td>sophos.skype.com.tw</td>
<td>?</td>
</tr>
<tr>
<td>Gorillaservers Inc.</td>
<td>Los Angeles, USA</td>
<td>198.100.96.0 - 198.100.127.255</td>
<td>198.100.121.15</td>
<td>margo.skype.com.tw</td>
<td>2013-11-22</td>
</tr>
<tr>
<td>Webnx Inc.</td>
<td>Los Angeles, USA</td>
<td>216.18.192.0 - 216.18.223.255</td>
<td>216.18.208.4</td>
<td>botemail.skype.com.tw</td>
<td>2013-04-04/2013-12-16</td>
</tr>
<tr>
<td>Webnx Inc.</td>
<td>Los Angeles, USA</td>
<td>216.18.192.0 - 216.18.223.255</td>
<td>216.18.208.4</td>
<td>qinoo.skype.com.tw</td>
<td>?</td>
</tr>
<tr>
<td>Data Communication Business Group</td>
<td>Taipei, Taiwan</td>
<td>59.112.0.0 - 59.123.255.255</td>
<td>59.120.84.230</td>
<td>botemail.skype.com.tw</td>
<td>2012-03-12/2012-04-28</td>
</tr>
<tr>
<td>Data Communication Business Group</td>
<td>Taipei, Taiwan</td>
<td>211.75.128.0 - 211.75.255.255</td>
<td>211.75.195.1</td>
<td>super.skype.com.tw</td>
<td>2011-08-30/2013-12-16</td>
</tr>
</tbody>
</table>

---

Copyright © 2014 Airbus Defence & Space - All rights reserved
### Operation Pitty Tiger – “The Eye of the Tiger”

**Data Communication Business Group**
Taipei, Taiwan  
61.220.0.0 - 61.227.255.255  
61.220.44.244  
aniu.skypetm.com.tw  
2013-04-05/2013-12-16

**Data Communication Business Group**
Taipei, Taiwan  
61.220.0.0 - 61.227.255.255  
61.220.44.244  
zeng.skypetm.com.tw  
?

**Data Communication Business Group**
Taipei, Taiwan  
61.220.0.0 - 61.227.255.255  
61.220.209.17  
qinoo.skypetm.com.tw  
?

**New World Telephone Ltd.**
Hong Kong City, Hong Kong  
113.10.169.0 - 113.10.169.255  
113.10.169.162  
margo.skypetm.com.tw  
Actually in use

**New World Telephone Ltd.**
Hong Kong City, Hong Kong  
58.64.185.0 - 58.64.185.255  
58.64.185.200  
zeng.skypetm.com.tw  
2013-12-16/2013-12-16

**New World Telephone Ltd.**
Hong Kong City, Hong Kong  
113.10.240.0 - 113.10.240.255  
113.10.240.54  
qinoo.skypetm.com.tw  
?

**New World Telephone Ltd.**
Hong Kong City, Hong Kong  
113.10.221.0 - 113.10.221.255  
113.10.221.126  
zeng.skypetm.com.tw  
?

**New World Telephone Ltd.**
Hong Kong City, Hong Kong  
113.10.240.0 - 113.10.240.255  
113.10.240.50  
link.skypetm.com.tw  
2012-12-21/2013-12-16

**Asia Data (hong Kong) Limited**
Hong Kong City, Hong Kong  
101.1.17.0 - 101.1.31.255  
101.1.25.74  
zeng.skypetm.com.tw  
Actually in use

**Isp Satellite Broadband Provider**
Hong Kong City, Hong Kong  
202.174.130.0 - 202.174.130.255  
202.174.130.110  
ms11.skypetm.com.tw  
2011-02-27/2013-12-16

**Jeongkyunghee**
Anyang, South Korea  
221.144.0.0 - 221.168.255.255  
221.150.164.114  
link.skypetm.com.tw  
2011-06-29/2012-12-18

### COMMON CHARACTERISTICS BETWEEN THE TWO DOMAINS

**Malware families and samples**

Avstore.com.tw and skypetm.com.tw have 4 malware families in common, communicating to subdomains of both domains:
Links between malware samples, IP addresses and c&cs associated to avstore.com.tw and skypetm.com.tw

**OTHER DOMAINS LINKED WITH THE PITTY TIGER GROUP**

<table>
<thead>
<tr>
<th>Domain</th>
<th>Shares</th>
<th>with</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>webconference.com.tw</td>
<td>Whois information</td>
<td>techsun.com.tw</td>
<td></td>
</tr>
</tbody>
</table>

Public release
Threat Intelligence

“The Eye of the Tiger”
### IP Address:
- techsun.com.tw,
- trendmicro.org.tw

### stareastnet.com.tw
- **Whois information**
  - acers.com.tw,
  - foxcom.com.tw,
  - dopodo.com.tw,
  - pacific.com

- **IP Address**
  - dopodo.com.tw,
  - foxcom.com.tw,
  - kimoo.com.tw,
  - symantecs.com.tw

- **Notes**
  - Two PittyTiger malware and a CT RAT have been pointing to several stareastnet.com.tw subdomains.

### symantecs.com.tw
- **Whois information**
  - trendmicrogroup.com

- **IP Address**
  - dopodo.com.tw,
  - foxcom.com.tw,
  - kimoo.com.tw,
  - stareastnet.com.tw,
  - wmdshr.com,
  - trendmicro.org.tw

- **Notes**
  - A pittytiger dropper, a Paladin malware and a CT RAT have been pointing to several symantecs.com.tw subdomains.

### trendmicrogroup.com
- **Whois information**
  - symantecs.com.tw

### trendmicro.org.tw
- **Whois information**
  - Skypetm.com.tw,
  - avstore.com.tw

- **IP Address**
  - webconference.com.tw,
  - techsun.com.tw,
  - skypetm.com.tw,
  - kimoo.com.tw,
  - symantecs.com.tw,
  - wmdskip.com

- **Notes**
  - A paladin and a PittyTiger malware have been pointing to several trendmicro.org.tw subdomains.

### lightening.org.tw
- **Whois information**
  - helosaf.com.tw,
  - seed01.com.tw

- **IP Address**
  - webconference.com.tw,
  - techsun.com.tw,
  - trendmicro.org.tw

- **Notes**
  - Paladin and PittyTiger samples has been pointing to several lightening.org.tw subdomains.

### techsun.com.tw
- **Whois information**
  - webconference.com.tw

- **IP Address**
  - webconference.com.tw,
  - trendmicro.org.tw

### dopodo.com.tw
- **Whois information**
  - acers.com.tw,
  - foxcom.com.tw,
  - stareastnet.com.tw

- **IP Address**
  - stareastnet.com.tw,
  - symantecs.com.tw,
  - kimoo.com.tw

### foxcom.com.tw
- **Whois information**
  - acers.com.tw,
  - dopodo.com.tw,
  - stareastnet.com.tw

- **IP Address**
  - stareastnet.com.tw,
  - symantecs.com.tw,
  - kimoo.com.tw

### acers.com.tw
- **Whois information**
  - acers.com.tw,
  - foxcom.com.tw,
  - stareastnet.com.tw

- **IP Address**
  - symantecs.com.tw,
  - wmdshr.com,
  - kimoo.com.tw

---

*Links between domains used by Pitty Tiger*
Some domains registered by the group are very old. There is an increase in the registrations from 2010 on. All the e-mail addresses used are connected to the Pitty Tiger group.
VICTIMS

Mapping the victims of such a targeted campaign is not an easy task.

We have found the Pitty Tiger group to be very active against one particular private company from the defense industry and one academic network of a government, yet we think it was done to be used as a proxy for some of the group's operations.

We have also found some connections from other companies to the c&c servers, yet we did not find evidence that they were real victims.

These alleged victims do work in different sectors and are located mostly in European countries.

- 1 company from the defense industry;
- 1 company from the energy industry;
- 1 company from the telecommunications industry;
- 1 company specialized in web development.

It might be surprising to see a company specialized in web development here, yet it has built websites for interesting potential targets. We suspect Pitty Tiger to use this compromise to spearphish other companies which are in commercial relation with this web development company.

We have to mention that we only had access to three of the several attackers' servers. Therefore, we suppose the Pitty Tiger group could have more targets than what we could confirm.

We also found a lot of vulnerability scanners launched by the attackers at different targets, yet there was no sign of compromise.

During the course of our investigations, we discovered a RAR archive on the attacker’s server containing 5 Word documents and one small C source code. These documents belong to the defense company which has been compromised. According to the name of the files and the general feel of the archive, we do think it was extracted by the attackers to “show” someone what kind of data they could get from the compromise of that particular target. The documents were still exhibiting comments from various users, showing it was an ongoing work and not old documents.

Interestingly enough, we saw a part of these documents appear on Virus-Total, with an additional “gift” from the attackers, a payload dropping a malware.

There are only two options we can think of here:

- Someone from the same company has been targeted with this document.
- Someone from another company has been targeted with this document. This other company could be a partner or competitor.

Since we were unable to determine the intended use of this specific document, we can only suppose that it could be used to provide commercial advantages to competitors of that company, or used by a foreign state.
ATTACKERS

During our investigation, we found out interesting information about the Pitty Tiger group itself. After analyzing the various collected elements, we have tried to draw a portrait of this particular threat.

ATTACKER’S CONNECTIONS TO THE C&C

We have been able to get all the RDP connections logs to one c&c server:

<table>
<thead>
<tr>
<th>COMPUTER NAME</th>
<th>OCCURRENCES</th>
<th>IP ADDRESSES</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>50PZ80C-1DFDCB8</td>
<td>65</td>
<td>23.226.178.162</td>
<td>USA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>27.155.90.80</td>
<td>China</td>
</tr>
<tr>
<td></td>
<td></td>
<td>27.155.110.81</td>
<td>China</td>
</tr>
<tr>
<td></td>
<td></td>
<td>27.156.49.223</td>
<td>China</td>
</tr>
<tr>
<td></td>
<td></td>
<td>58.64.177.60</td>
<td>Hong Kong</td>
</tr>
<tr>
<td></td>
<td></td>
<td>59.53.91.33</td>
<td>China</td>
</tr>
<tr>
<td></td>
<td></td>
<td>103.20.192.11</td>
<td>Hong Kong</td>
</tr>
<tr>
<td></td>
<td></td>
<td>110.90.60.250</td>
<td>China</td>
</tr>
<tr>
<td></td>
<td></td>
<td>110.90.61.69</td>
<td>China</td>
</tr>
<tr>
<td></td>
<td></td>
<td>110.90.62.185</td>
<td>China</td>
</tr>
<tr>
<td></td>
<td></td>
<td>120.32.113.97</td>
<td>China</td>
</tr>
<tr>
<td></td>
<td></td>
<td>120.32.114.209</td>
<td>China</td>
</tr>
<tr>
<td></td>
<td></td>
<td>121.204.33.130</td>
<td>China</td>
</tr>
<tr>
<td></td>
<td></td>
<td>121.204.33.153</td>
<td>China</td>
</tr>
<tr>
<td></td>
<td></td>
<td>183.91.52.230</td>
<td>Hong Kong</td>
</tr>
<tr>
<td>FLY-THINK</td>
<td>11</td>
<td>27.151.0.224</td>
<td>China</td>
</tr>
<tr>
<td></td>
<td></td>
<td>27.155.109.89</td>
<td>China</td>
</tr>
<tr>
<td></td>
<td></td>
<td>121.204.88.120</td>
<td>China</td>
</tr>
<tr>
<td></td>
<td></td>
<td>120.32.114.139</td>
<td>China</td>
</tr>
<tr>
<td>TIEWEISHIPC</td>
<td>2</td>
<td>27.16.139.143</td>
<td>China</td>
</tr>
<tr>
<td>CHMXY-PC</td>
<td>1</td>
<td>58.61.40.5</td>
<td>China</td>
</tr>
</tbody>
</table>

*RDP connections from attackers machines to one particular c&c, from beginning of April 2014 to beginning of July 2014*

These connections are either VPS or dynamic IP addresses, mostly from China.

A computer named CHMXY-PC connected to the c&c via RDP with IP address 58.61.40.5. The IP is in an ADSL dynamic pool in the Gangzhou area (Guangdong province):
A few connections to the c&c were done by a computer named TIEWEISHIPC with IP address 27.16.139.143. This IP address belongs to an ADSL dynamic pool in the Wuhan area (Hubei’s provincial capital).

Some connections to the c&c originated from a computer named FLY-THINK with several IP addresses, all located in Fuqing (Fujian province). The IP addresses are in an ADSL dynamic pool:
Most of the connections to the c&c server were coming from a computer named 50PZ80C-1DFDCB8 with several IP addresses. There are 11 IP addresses from Chinese dynamic ADSL ranges: 9 from Fuqing (Fujian province), one from Fuzhou (Fujian’s province capital) and one from Nanchang (Jiangxi’s province capital). The last one came from a VPS instance located in Los Angeles (California, USA) but purchased by a China based VPS provider XeVPS which belong to the AS38197 (Sun Network Hong Kong Limited).
The two computers FLY-THINK and 50PZ80C-1DFDCB8 have used distinct IP addresses to connect to the C&C, yet some of these IP addresses come from the same IP range:

We mapped these RDP connections to have a graphical view:
RDP connections from the attackers to one c&c server

“TooT”

We found that a member of this group of attackers used some tools on his own system, for testing purposes. This information was still available when we got access to the c&c server.

He launched some tests with the CT RAT we exposed earlier:

```
2014-02-10 09:48:29
Login
->C:toot-2a601225a8
->U:Toot
->L:10.10.10.113
->S:Microsoft Windows XP Service Pack 3 5.1.2600
->M:Nov 13 2013
->P:1028  OBTIA(1$1$)

C:\Documents and Settings\Administrator>
```

User “Toot” logging on the CT RAT on machine “toot-2a601225a8”, 2014/02/10
Here we can see a user “Toot” from a machine named “toot-2a601225a8” logging in the CT RAT and executing some commands. The c&c IP address, 198.100.113.27, can be seen there. Other log files showed that “Toot” is using virtual machines for his tests.

We can also see the system: Microsoft Windows XP SP3. The “P” field is the language ID.
1028 means “Chinese traditional”. We have also seen tests run by “toot” with a language ID of 2052, which is “Chinese simplified”.

The “M” field is probably used for versioning. It is a hardcoded string in the binary.

After these tests, we could see some real connections to a victim using this RAT. Here is a follow-up of the commands launched by the bot controller, in a standard command-line shell:

<table>
<thead>
<tr>
<th>Command</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>cd\temp</td>
<td>Folder change</td>
</tr>
<tr>
<td>Dir</td>
<td>Lists the content of the folder. The attacker here is probably looking for his tools and does not remember if they are there or in system32.</td>
</tr>
<tr>
<td>cd\windows\system32</td>
<td>Folder change</td>
</tr>
<tr>
<td>dir tools*</td>
<td>Looking for tools.exe, a tool to fetch different kind of credentials on the system</td>
</tr>
<tr>
<td>tools</td>
<td>The attacker wants to see what the options are for the tool.</td>
</tr>
<tr>
<td>tools –all</td>
<td>Tools.exe is launched. At this point, the output shows the attackers only gets successfully one MSN credential in clear text, login and password, and one Microsoft Outlook credential.</td>
</tr>
<tr>
<td>type iecache.txt</td>
<td>Shows the Internet Explorer cache to the attacker. The output is huge.</td>
</tr>
<tr>
<td>dir cmd.exe</td>
<td>Looking for cmd.exe</td>
</tr>
<tr>
<td>del tools.exe</td>
<td>Remove the tools.exe after its use</td>
</tr>
<tr>
<td>dir tools.exe</td>
<td>Checks to see if it has been successfully deleted</td>
</tr>
<tr>
<td>del iecache.txt</td>
<td>Removes the IE cache log file.</td>
</tr>
<tr>
<td>regedit -e 1.reg</td>
<td>Dumps the content of this key to a file named 1.reg</td>
</tr>
<tr>
<td>&quot;HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows&quot;</td>
<td></td>
</tr>
<tr>
<td>type 1.reg</td>
<td>Checks if dump has been successful.</td>
</tr>
<tr>
<td>del 1.reg</td>
<td>Deletes the dump</td>
</tr>
<tr>
<td>regedit -e v1.reg</td>
<td>Do it again, we do not know why the attacker does this the output is the same as for previous regedit command</td>
</tr>
<tr>
<td>&quot;HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows&quot;</td>
<td></td>
</tr>
<tr>
<td>type v1.reg</td>
<td>Checks the dump again</td>
</tr>
<tr>
<td>dir *.reg</td>
<td>Looking for traces left in this folder</td>
</tr>
<tr>
<td>del v1.reg</td>
<td>Deletes the one *.reg file left.</td>
</tr>
<tr>
<td>del c:\windows\system32\mfqtirq.exe</td>
<td>Removes a binary used in the attack</td>
</tr>
<tr>
<td>del c:\windows\system32\crupalo.dll</td>
<td>Removes a binary used in the attack</td>
</tr>
<tr>
<td>dir c:\windows\system32\mfqtirq.exe</td>
<td>Checks if removal has been successful</td>
</tr>
<tr>
<td>dir c:\windows\system32\crupalo.dll</td>
<td>Checks if removal has been successful</td>
</tr>
</tbody>
</table>
The attacker goes on like this, using his tools, and then ends the communication with this RAT on that computer.

Please note that at this point, the attacker has at least the privileges of a local administrator, since he is allowed to write content in the system32 folder of a Windows XP system. He could also gain the credentials to a sensitive e-mail account.

In addition to all information already shown, we saw Toot connect to an account on a cloud service named “Baidu Drive”. The e-mail address linked to this account is dyanmips@qq.com (QQ-ID: 2589315828). We could find traces of two other e-mail accounts associated to Toot, cisco_dyanmips@qq.com (QQ ID: 204156335) and cisco_dynamips@qq.com (QQ ID: 1878836793).

We did not find more information about user “Toot”, yet we miss Chinese language capabilities.
“Cold & Snow”

The controller part of CT RAT/PittyTiger RAT revealed the following “about” information, once translated from Chinese to English language:

CT console (compatible pittytiger) v1.3
2013.12 by Trees and snow

We believe this translation of the author’s name might not be accurate due to the use of automated translation tools. Moreover, we have strong suspicions that there is not a single individual nicknamed “Trees and snow” but rather two programmers nicknamed “Trees” and “Snow”. “Trees” could also be “Cold”. We noticed that the symbol for this word is translated differently according to the context it is used in. Once again, we lack Chinese language skills.

We identify the two nicknames on the current campaign as Autumn Snow (秋雪) and Cold Air Kiss (风吻寒).

While we are confident that these people are indeed the developers of both PittyTiger and CT RAT malware, we are not sure they belong to the PittyTiger group. These developers might just have been hired to develop these RATs. They might also just be selling it to the PittyTiger group. There is no trace of usage from other attacking groups, we believe the PittyTiger RAT is exclusively used by this group of attackers.

Roles and Organization

According to indicators we gathered and threat activities profiling we have some hypotheses on the way the group is conducting its operations.

We have strong evidence of a bot operator position. We identify one nickname for this position, the user known as TooT. As we did not see other nickname, we think that TooT is one person and not a group of persons.

We also identified a malware development position. We identified two nicknames for this position on the current campaign, Autumn Snow (秋雪) and Cold Air Kiss (风吻寒). Yet we are unsure that they belong to the group, they might just be a third party providing or selling their malware.

We have a strong suspicion of a coordinator position, which coordinates the bot operator, provides him with some logistics support (weaponized document, tools…) and reviews the programmers work. This position could imply a communication channel with another manager.
We named this position ‘Chen’, in relation with several references of this common Chinese name in c&c WHOIS and other investigation materials.

We have some suspicion of a customer relationship manager position that may act as an interface between a customer and Chen. We named this position ‘Lilly’.
ATTACKERS ARSENAL

The c&c servers used by the attackers revealed a lot of interesting files stored in various folders:

<table>
<thead>
<tr>
<th>Filename</th>
<th>Description</th>
<th>Public tool?</th>
</tr>
</thead>
<tbody>
<tr>
<td>32m.exe / 3200.exe / 32mm.exe / mm32.exe</td>
<td>MM RAT</td>
<td>No</td>
</tr>
<tr>
<td>iupdate.exe / insert.exe / khuvaxu.exe</td>
<td></td>
<td></td>
</tr>
<tr>
<td>322.exe</td>
<td>Chinese version of calc.exe, probably for testing purposes</td>
<td>Yes</td>
</tr>
<tr>
<td>client.exe</td>
<td>File transfer tool, via pipes</td>
<td>No</td>
</tr>
<tr>
<td>CP.exe/CP_sep.exe</td>
<td>Microsoft Outlook dumper</td>
<td>No</td>
</tr>
<tr>
<td>CT.exe</td>
<td>Controller for CT RAT (2013.10)</td>
<td>No</td>
</tr>
<tr>
<td>ct1.exe</td>
<td>Controller for both CT RAT and PittyTiger RAT</td>
<td>No</td>
</tr>
<tr>
<td>Diruse.exe</td>
<td>Tool to display disk usage for a directory tree</td>
<td>Yes</td>
</tr>
<tr>
<td>GlobalWind.exe</td>
<td>Controller for Pitty Tiger</td>
<td>No</td>
</tr>
<tr>
<td>gsec1.exe</td>
<td>GSecDump password dumper</td>
<td>Yes</td>
</tr>
<tr>
<td>http.exe/wsup.exe</td>
<td>Controller for MM RAT</td>
<td>No</td>
</tr>
</tbody>
</table>
### Operation Pitty Tiger – “The Eye of the Tiger”

<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>km.exe</td>
<td>“Toyi” keylogger</td>
<td>No</td>
</tr>
<tr>
<td>logreader.exe</td>
<td>Tool to decrypt the km.exe keylogger data</td>
<td>No</td>
</tr>
<tr>
<td>Mailpv.exe</td>
<td>“Mail PassView” tool, to extract e-mail passwords from various e-mail clients.</td>
<td>Yes</td>
</tr>
<tr>
<td>Netpass.exe</td>
<td>“Network Password Recovery” tool, to extract network passwords.</td>
<td>Yes</td>
</tr>
<tr>
<td>iepv.exe /iepv-jiake.exe</td>
<td>“IE PassView” tool, to extract passwords from Internet Explorer. The file iepv-jiake.exe is the same, but crypted using a tool named DarkCrypt (DarkCrpt).</td>
<td>Yes</td>
</tr>
<tr>
<td>routerpass.exe</td>
<td>“Router PassView” tool, to extract credentials in some router backup files.</td>
<td>Yes</td>
</tr>
<tr>
<td>pstpass.exe</td>
<td>“PstPassword” tool, to extract Outlook’s PST files passwords.</td>
<td>Yes</td>
</tr>
<tr>
<td>vncpass.exe</td>
<td>“VNCPassView” tool, to extract passwords stored by the VNC tool.</td>
<td>Yes</td>
</tr>
<tr>
<td>rdpv.exe</td>
<td>“Remote Desktop PassView” tool, to extract the passwords from .RDP files.</td>
<td>Yes</td>
</tr>
<tr>
<td>lookpass.exe</td>
<td>Password revealer.</td>
<td>Yes</td>
</tr>
<tr>
<td>tools.exe, res.exe</td>
<td>Multi password dumper: RDP, VNC, IE, ProtectedStorage, MSN, Wireless, etc.</td>
<td>No</td>
</tr>
<tr>
<td>p2012.exe</td>
<td>Controller for Paladin 2.1</td>
<td>No</td>
</tr>
<tr>
<td>p.exe</td>
<td>Controller for Paladin 2.2</td>
<td>No</td>
</tr>
<tr>
<td>po.exe</td>
<td>TCP Tunneling tool.</td>
<td>No</td>
</tr>
<tr>
<td>pp.exe</td>
<td>Controller for Paladin 2.1</td>
<td>No</td>
</tr>
<tr>
<td>pr.exe</td>
<td>Dotpot port scanner.</td>
<td>Yes</td>
</tr>
<tr>
<td>rar.exe</td>
<td>Rar archiving tool, command-line version.</td>
<td>Yes</td>
</tr>
<tr>
<td>sff.exe</td>
<td>File-searching tool to hunt for doc, txt, mdb, sec, eml, vsd, ppt, pps, dbx (SearchFile).</td>
<td>No</td>
</tr>
<tr>
<td>ssqlexe</td>
<td>MySQL scanner.</td>
<td>No</td>
</tr>
<tr>
<td>w7ij32.exe</td>
<td>Windows 7 DLL injector.</td>
<td>No</td>
</tr>
<tr>
<td>ToyI.dll</td>
<td>Keylogger. Can be used with w7ij32.exe</td>
<td>No</td>
</tr>
<tr>
<td>winspre.exe</td>
<td>Troj/ReRol.A</td>
<td>No</td>
</tr>
<tr>
<td>dr.asp</td>
<td>Front-end for Troj/ReRol.A</td>
<td>No</td>
</tr>
<tr>
<td>sk.exe</td>
<td>Snake’s SkServer.</td>
<td>Yes</td>
</tr>
<tr>
<td>Fluxay5Beta1</td>
<td>Vulnerability scanner</td>
<td>Yes</td>
</tr>
<tr>
<td>feitafanghuoqiang</td>
<td>Fortinet vulnerability scanner</td>
<td>No</td>
</tr>
<tr>
<td>Hscan1.2</td>
<td>Vulnerability scanner</td>
<td>Yes</td>
</tr>
<tr>
<td>mimi.exe, mimikaz64.exe</td>
<td>Mimikatz password dumper</td>
<td>Yes</td>
</tr>
<tr>
<td>o2scan</td>
<td>Vulnerability scanner</td>
<td>Yes</td>
</tr>
<tr>
<td>Openssl</td>
<td>Heartbleed Exploit</td>
<td>Yes</td>
</tr>
<tr>
<td>X-Scan-v3.3</td>
<td>X-Scan vulnerability scanner</td>
<td>Yes</td>
</tr>
<tr>
<td>8uFTP</td>
<td>FTP client</td>
<td>Yes</td>
</tr>
<tr>
<td>NcFTP</td>
<td>FTP client</td>
<td>Yes</td>
</tr>
<tr>
<td>SEPM exploit</td>
<td>Remote command execution exploit on Symantec Endpoint Protection Manager (CVE-2013-5014, CVE 2013-5015)</td>
<td>Yes</td>
</tr>
</tbody>
</table>
This is quite the usual arsenal for a group of APT attackers:

- Malware (Troj/ReRol.A)
- Remote Administration Tools (MM RAT, CT RAT, Pitty Tiger, Paladin)
- E-mail espionage tools (cp.exe, mailpv.exe)
- Passwords dumpers (gsecdump, NirSoft tools, Mimikatz etc.)
- Network scanners (pr.exe)
- Network-oriented tools (po.exe)
- Vulnerability scanners (ssql.exe, Fluxay, etc.)

What is rare to find is the controller part of those tools. We have been lucky enough to get the controller part of Pitty Tiger and CT RAT, and even to get a kind of hybrid controller made for CT RAT but also supporting Pitty Tiger. We suppose that the CT RAT is the new evolution of Pitty Tiger and that it will replace Pitty Tiger in the following months.

The presence of a Chinese version of “calc.exe”, the official calculator provided in Microsoft Windows, is interesting. Not only is it one more indicator of a probable Chinese origin, but also an indicator that this server was probably used as a test base, in addition to being operational and controlling infected machines from different targets.

In addition to those tools, we found some interesting scripts. A script named ipc.bat uses a file named user.txt to try to brute-force a shared folder access:

```bash
for /f "tokens=1,2 delims= " %i in (user.txt) do (net use \<TARGETEDIP>\ipc$ "%%j" /u:%%i) && (net use \<TARGETEDIP> /del) && (echo user:%%i pass:%%j>>succ.txt)
```

One script used to brute-force a network share inside a company’s network

The user.txt file contains thousands of lines, each one being a couple of one particular username and one password attempt:

```
administrator nameofonetargetedcompany
administrator !Password
administrator azerty123
...
administrateur nameofonetargetedcompany
administrateur !Password
administrateur azerty123
...
<username>nameofonetargetedcompany
<username> !Password
<username> azerty123
...
<anotheruser>nameofonetargetedcompany
<anotheruser> !Password
<anotheruser> azerty123
...
```

Anonymized dictionary file used for brute-forcing a network share
This user.txt file has been anonymized, yet we wanted to give you the feel for it. This file is 67320 lines long, and uses 5610 different passwords for each of 12 users contained in this file. The user names are clearly the result from a user enumeration and are dedicated to a particular French victim.

The passwords listed in this file are either build from several campaigns or from the current campaign. A lot of passwords are related to the targeted company and might be previous passwords from users.

We have also discovered a pack of files which can be used to trigger an Internet Explorer vulnerability (CVE-2014-0322). The date of these files, namely Tope.swf and index.html, was 2014/02/18, a few days after the revelation of existing exploits in the wild used in APT attacks\(^1\).

We do not know if the Pitty Tiger group used this exploit or not, but found no trace indicating they did. A lot of different attackers seem to have used that vulnerability since.

\(^1\)http://www.symantec.com/connect/blogs/new-internet-explorer-10-zero-day-discovered-watering-hole-attack
ATTRIBUTION

Determining who is exactly behind an APT campaign is difficult. We tried to extract different technical indicators, together with contextual elements.

Information relating to the tools used by the attackers has been leveraged for attribution:

- Several Chinese vulnerability scanners have been launched against targets;
- Several Chinese tools have been used and found on the c&c servers of the attackers: 8uFTP, a Chinese version of calc.exe, etc.;
- Two of the used RATs have been developed by the same developers: CT RAT and PittyTiger RAT. The controllers for these RATs show Chinese language;
- Several binaries used by the attackers show either “Chinese - China” or “Chinese-Taiwan” language ID in their resources;
- A decoy Word document has been found, written in Chinese language;

The IP addresses used for the hosting of the c&c domains are mainly located in Taipei (Taiwan) and Hong Kong City (Hong Kong Special Administrative Region, PRC):
Most RDP connections to the c&c infrastructure come from Chinese IP ranges in Fuqing (Fujian province, PRC). Yet some IP addresses in the USA and in Hong Kong have also been found;
All the items listed in this chapter are strong indicators that the attackers might be Chinese.
CONCLUSION

Pitty Tiger is a group of attackers that have been active since at least 2011.

Pitty Tiger is effective and mature in the use of targeted malware, the use of known exploits to infect computers with their malware and the creation of an infrastructure to efficiently conduct APT attacks.

They are quite unprofessional in their way of using their infrastructure: they do launch vulnerability scanners directly from a c&c server and also use their connection for personal activities (downloading pornographic material for example, as we have seen a whole folder on a c&c server full of xxx torrent links).

Pitty Tiger is probably not a state-sponsored group of attackers. The attackers lack the experience and financial support that one would expect from state-sponsored attackers. We suppose this group is opportunistic and sells its services to probable competitors of their targets in the private sector.

One governmental network has been targeted by the group, yet we do not have any evidence of the purpose of this attack. We suppose this particular attack has been executed to provide a usable bounce for the group.

The campaign we studied has been largely focused on one particular target. We suspect the Pitty Tiger group to work according to an opportunistic business model: this group might offer its services to third parties from the private sector.

This group seems to be very small compared to other APT groups. We have leveraged several profiles and could identify some attackers to a certain extent. We believe this group might keep working as it is now, with limited budgets, or grow to extend its attacking campaign capabilities.
INDICATORS

This list of indicators is provided in order to help people detect Pitty Tiger APT campaign.

DOMAINS

Domains used by the Pitty Tiger group: (please note several subdomains are used, as seen in the report)

acers.com.tw
kimoo.com.tw
pacific.com
foxcom.com.tw
dopodo.com.tw
trendmicroup.com
lightening.com.tw
avstore.com.tw
helosaf.com.tw
trendmicro.org.tw
stareastnet.com.tw
symantecs.com.tw
seed01.com.tw
skypetm.com.tw

MALWARE HASHES

<table>
<thead>
<tr>
<th>MD5 Hashes</th>
<th>Malware Family</th>
</tr>
</thead>
<tbody>
<tr>
<td>dc3d905ed90bcc148bcd34fe0c94d2d</td>
<td>PittyTiger RAT</td>
</tr>
<tr>
<td>dd87c68c1e71bb104a48a6be87a2349f</td>
<td></td>
</tr>
<tr>
<td>a494010a51705f7720d3cd378a31733a</td>
<td></td>
</tr>
<tr>
<td>be18418cafd89f86303f7e419a389cc9</td>
<td></td>
</tr>
<tr>
<td>0750569cf173344bb01169476387cc2</td>
<td></td>
</tr>
<tr>
<td>3282a5e77f24c645984ef152a2aee874</td>
<td></td>
</tr>
<tr>
<td>8a54adb3976d1c03605656ca55be7400</td>
<td></td>
</tr>
<tr>
<td>666ae21ceaa9bb8017a967ea6128add</td>
<td></td>
</tr>
<tr>
<td>a1ea6dc12b983c7262fe76c1b3663b24</td>
<td></td>
</tr>
<tr>
<td>d5da60f67d5a55a847e1e6723c7a4d0</td>
<td></td>
</tr>
<tr>
<td>55e456339936a56c73a7883ea1ddb762</td>
<td></td>
</tr>
<tr>
<td>abb0abfab252e45bb9106273df3c1c2</td>
<td></td>
</tr>
<tr>
<td>4ab74387f7a02c115deea2110f961fd3</td>
<td>Troj/ReRol.A</td>
</tr>
<tr>
<td>b6380439ff9ed0c6d45759da0f3b05b8</td>
<td></td>
</tr>
<tr>
<td>bf95e89906b8a17fd611002660fff32</td>
<td></td>
</tr>
<tr>
<td>ce15fa3338b7fe780e85c511d5e49a98</td>
<td></td>
</tr>
<tr>
<td>5e2360a8c4a0ccee1ae22919d8bf49fd</td>
<td></td>
</tr>
<tr>
<td>12854b8d1e6a590e1bd578267e4f8c9</td>
<td></td>
</tr>
<tr>
<td>5e2360a8c4a0ccee1ae22919d8bf49fd</td>
<td></td>
</tr>
</tbody>
</table>
### Strings (File/Network)

<table>
<thead>
<tr>
<th>Data type</th>
<th>Malware Family</th>
</tr>
</thead>
<tbody>
<tr>
<td>File string / Network string</td>
<td>PittyTiger RAT</td>
</tr>
<tr>
<td>----PittyTiger</td>
<td>PittyTiger RAT</td>
</tr>
<tr>
<td>netsvcs_0x%d</td>
<td>Paladin RAT</td>
</tr>
<tr>
<td>\MSREVTS.RG</td>
<td>Paladin RAT</td>
</tr>
<tr>
<td>/httpdocs/mm/&lt;bot_id&gt;/ComMand.sec</td>
<td>MM RAT</td>
</tr>
<tr>
<td>/httpdocs/prx.sec</td>
<td>MM RAT</td>
</tr>
<tr>
<td>CmdShell closed.</td>
<td>MM RAT</td>
</tr>
<tr>
<td>get file ok %u bytes</td>
<td>CT RAT</td>
</tr>
<tr>
<td>ok sleep %d minutes.</td>
<td>CT RAT</td>
</tr>
<tr>
<td>can't open mmfile</td>
<td>Troj/ReRol.A</td>
</tr>
<tr>
<td>Mozilla/4.0 (compatible;)</td>
<td>Troj/ReRol.A</td>
</tr>
<tr>
<td>/dr.asp</td>
<td>Troj/ReRol.A</td>
</tr>
</tbody>
</table>

### Malware RATs

- Paladin RAT
- CT RAT
- MM RAT (aka Troj/Goldsun-B)
- Leo RAT