The Eye of the Tiger

By David Bizeul, Ivan Fontarensky, Ronan Mouchoux, Fabien Perigaud, Cedric Pernet on 2014/07/11, 11:00 - Investigation - Permalink

APT Pitty Tiger Publication Threat Intelligence White paper

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.

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 and enlights the activities of a structured organization working in the APT field.

You can get more information in our Whitepaper.

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 community.

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

Our researches around the malware family revealed the “Pitty Tiger” group has been active since 2011, yet we found traces which makes us believe the group is active since 2010.

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

- PittyTiger
- Troj/ReRol.A
- CT RAT
- MM RAT (aka Troj/Goldsun-B)
- Paladin RAT (a variant of Gh0st RAT)

Infection methods

The Pitty Tiger group mostly uses spear phishing in order to gain an initial foothold within the targeted environment. The group exploits known vulnerabilities in Microsoft Office products to infect their targets with malware.

Pitty Tiger group is sometimes using stolen material as spear phishing content to target other persons. They have also been seen using HeartBleed vulnerability in order to directly get valid credentials.

Malware information

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 (CVE-2012-0158). The group could also use CVE-2014-1761, which is more recent.

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.

Once compromised, PittyTiger rat is often installed. 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.

But things are changing. CT 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.

As a matter of fact, this group does neither use one favorite RAT nor two but many...

We named as “MM RAT” a specific code 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.

Paladin RAT is another remote administration tool used by the Pitty Tiger group. This malware is a variant of the infamous Gh0st RAT . Our specific sample uses “ssss0” instead of the usual “Gh0st” header for network communications. The commands ID used in the communication protocol have also changed, but the features are quite the same.

Additionally to the Paladin RAT previously mentionned, 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 is has been used by the group, in opposition to Paladin which is used often by Pitty Tiger.

INFRASTRUCTURE

Search

OK

Tags

log
anonymization
welcome
GoodFET
Z-Wave
side-channels
critical infrastructures
Hardware Trojans
Sakula
BlackVine
advanced persistent threat
ransomware
reconnaissance
bitcrypt
APT kill chain
PlugX
Advanced Persistent Threat
reverse engineering
malware
APT
All tags

Useful Links

Cybersecurity Job offers
AIRBUS D&S CyberSecurity
BitBucket CyberTools

Share

0

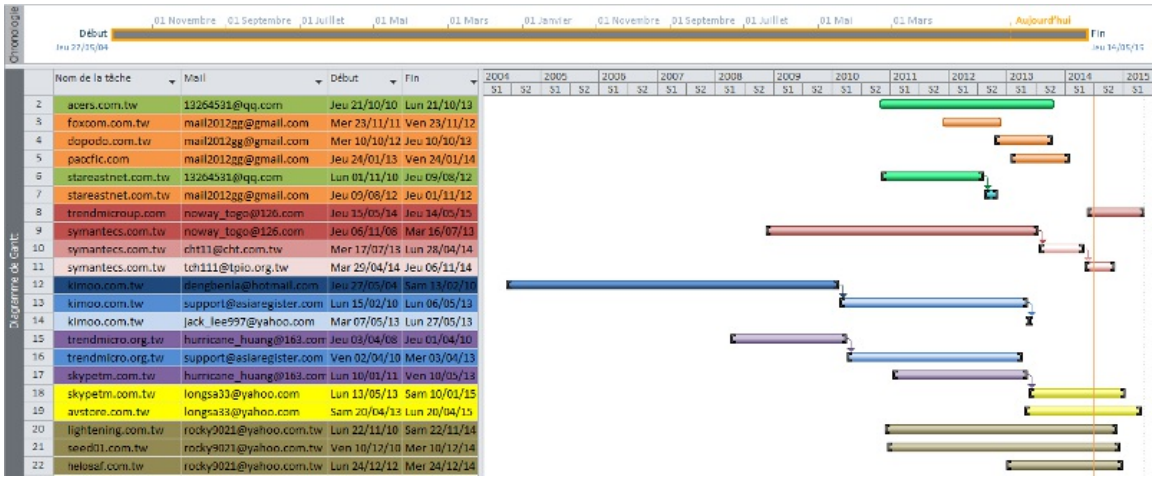
Subscribe

Entries feed

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, had one very common flaw: the attackers had misconfigured the access control of several folders. Once parsed and dumped, it provided us more insight.

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.

We have been able to list the main domains registered and used by Pitty Tiger as c&c servers:



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 supposed 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.

ATTACKERS

We found out interesting information about the Pitty Tiger group.

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

COMPUTER NAME	OCCURENCES	IP ADDRESSES	COUNTRY
50PZ80C-1DFDCB8	65	23.226.178.162	USA
		27.155.90.80	China
		27.155.110.81	China
		27.156.49.223	China
		58.64.177.60	Hong Kong
		59.53.91.33	China
		103.20.192.11	Hong Kong
		110.90.60.250	China
		110.90.61.69	China
		110.90.62.185	China
		120.32.113.97	China
		120.32.114.209	China
		121.204.33.130	China
		121.204.33.153	China
		183.91.52.230	Hong Kong
FLY-THINK	11	27.151.0.224	China
		27.155.109.89	China
		121.204.88.120	China
		120.32.114.139	China
TIEWEISHIPC	2	27.16.139.143	China
CHMXY-PC	1	58.61.40.5	China

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

ROLES AND ORGANIZATION

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

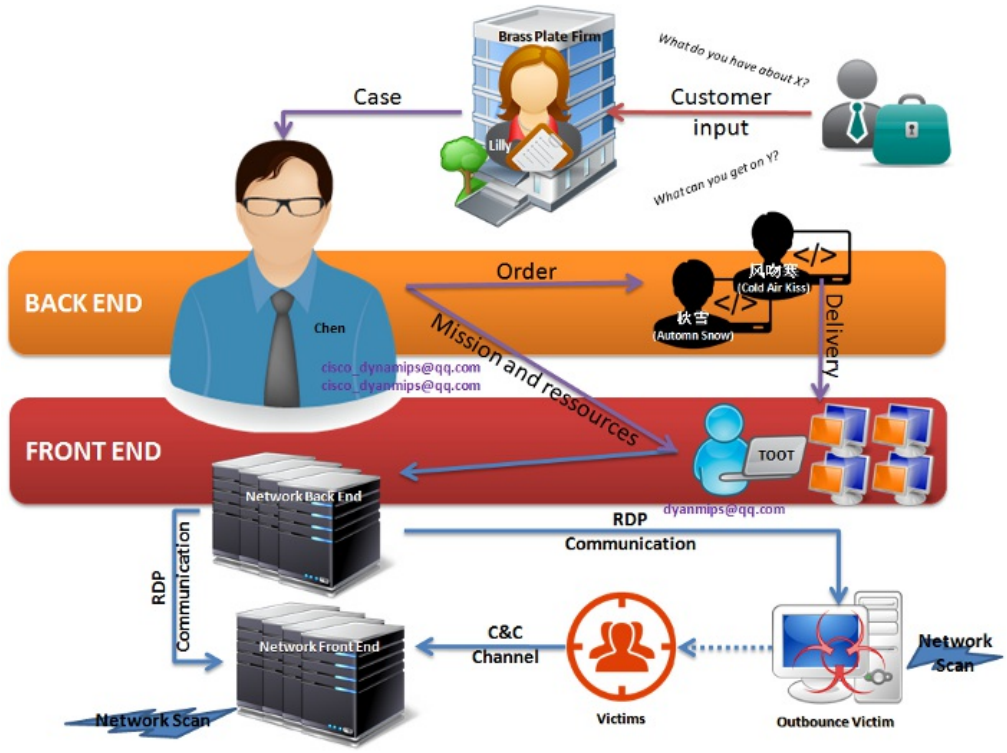
We have strong evidence of a bot operator position. We identify one nickname for this position, the user known as TooT. As we did not see other nickname, we think that TooT is one person and not a group of persons.

We also identified a malware development position. We identified two nicknames for this position on the current campaign, Automn 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’.



A proposal for Pitty Tiger team structure

ATTACKERS ARSENAL

The c&c servers used by the attackers revealed a lot of interesting files stored in various folders, building a real attackers arsenal of malware and tools:

- 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.

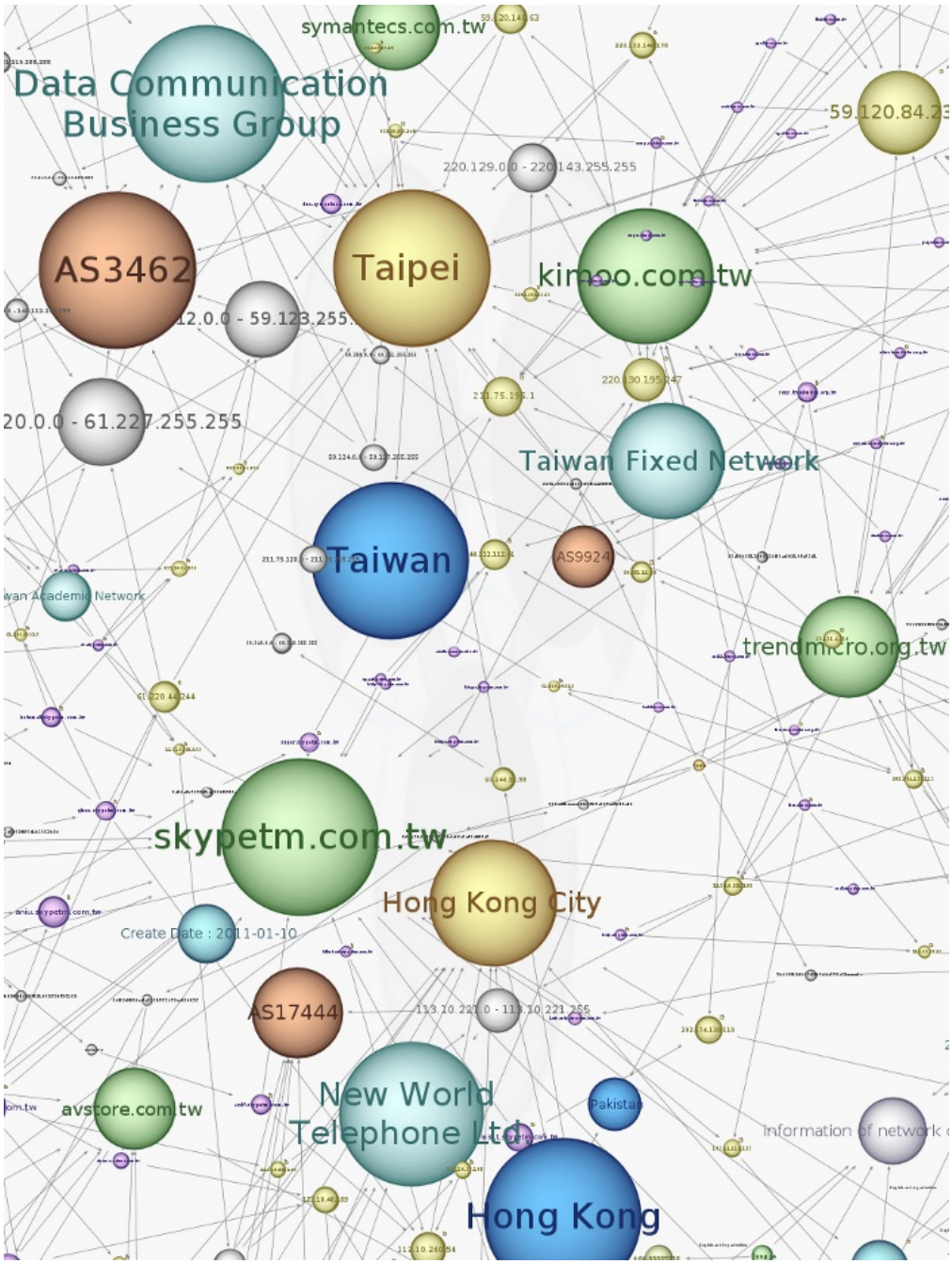
ATTRIBUTION

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 (Taïwan) and Hong Kong City (Hong Kong Special Administrative Region, PRC):



All the items listed in this part are strong indicators that the attackers might be Chinese.

Read the full Whitepaper for more information