APT1: One of China's Cyber Espionage Units

In the Information Age it won't sound far-fetched, if we're told that an entity is involved in Cyber Espionage at a Global Scale. But it's a whole other story if we're told that this Cyber Espionage is funded by the government of an Emerging Economy.

Mandiant is a Security Company that investigates Cyber Security Breaches around the world. Much of these Security Breaches are caused by 'Advanced Persistant Threats' (a term coined by the US Air Force in 2006), meaning that these threat actors have advanced capabilities and they are obstinate in the face of Security.

In January 2010 Mandiant published an interesting theory that these APTs may be funded by the Chinese Government however they did not have sufficient evidence to prove it. In 2013, Mandiant published another report on 'APT1' which primarily blames the Chinese Government to be involved in funding Cyber Espionage activities around the Globe and contains the supporting technical evidence.

Mandiant's VP says "We've provided all the evidence here. This is something our industry needs to do more of, Mandiant is proud to participate in this kind of information sharing. We are not issuing a one page baseless accusation; we're providing 60 pages of evidence and over 3000 technical indicators like IP Addresses, domain names and encryption certificates. We welcome scrutiny and invite other researchers to take a look at the evidence and we are confident they will arrive to the same conclusion."

Gist of the Mandiant Report:

- There are more than 20 APT Groups in China, however the report focuses on one of them (referred to as APT1) which is the most prolific one.
- APT1 has direct Government support and it is similar in its characteristics as the PLA's Unit 61398 of the Chinese Army and has the same location.
- This Unit 31698 is located at Datong Road, Pudong New Area of Shanghai.
- This building which is estimated to be inhabited by 1000s of People, is a 130,663 square foot facility and has 12 stories (see figure).

Figure 1: APT1 Building (Source: Mandiant APT1 Report)

- Special fiber optic Communication facilities are provided for this unit in the name of national defense. Mandiant was able to locate a scanned China Telecom memo over the Internet which talked about approval for providing the 'requested channel'since this is concerning "defense construction".
- The professionals inside the building are trained in computer Security (the APT1 Actors) and have proficiency in the English language (these APT Actors need to carry out Social Engineering attacks like formulating a Spear Phishing Email that requires clever use of the English language since mostly English Speaking countries are targeted). This is a stable day job for them.

Facts about the APT1:

- APT1 establish min. of 937 Command and Control (C2) servers
  - hosted on 849 distinct IP addresses in 13 countries.
  - Majority were registered to organizations in China (709)
  - followed by the U.S. (109)
- In the last several years mandiant have confirmed 2,551 FQDNs attributed to APT1
- Between January 2011 and January 2013 Mandiant confirmed
  - 1,905 instances of APT1 actors using their attack infrastructure
  - from 832 different IP addresses

Largest APT1 data theft from a single organization:

6.5 Terabytes

over 10 months

Longest time period within which APT1 has continued to access a victim's network:

4 Years, 10 Months

Figure 2: Noted APT1 Victims over the years (Source: Mandiant APT1 Report)

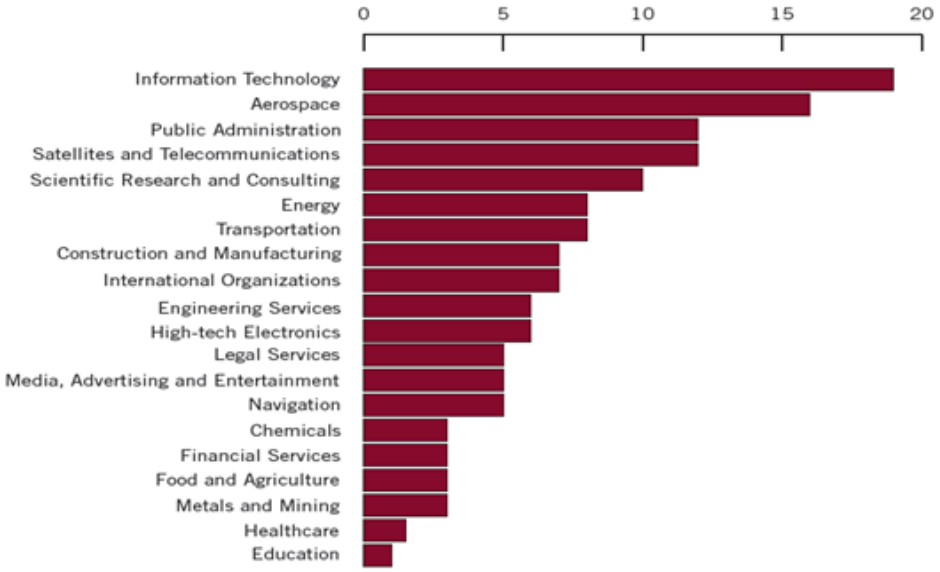

Figure 3: Industries compromised by APT1 (Source: Mandiant APT1 Report)

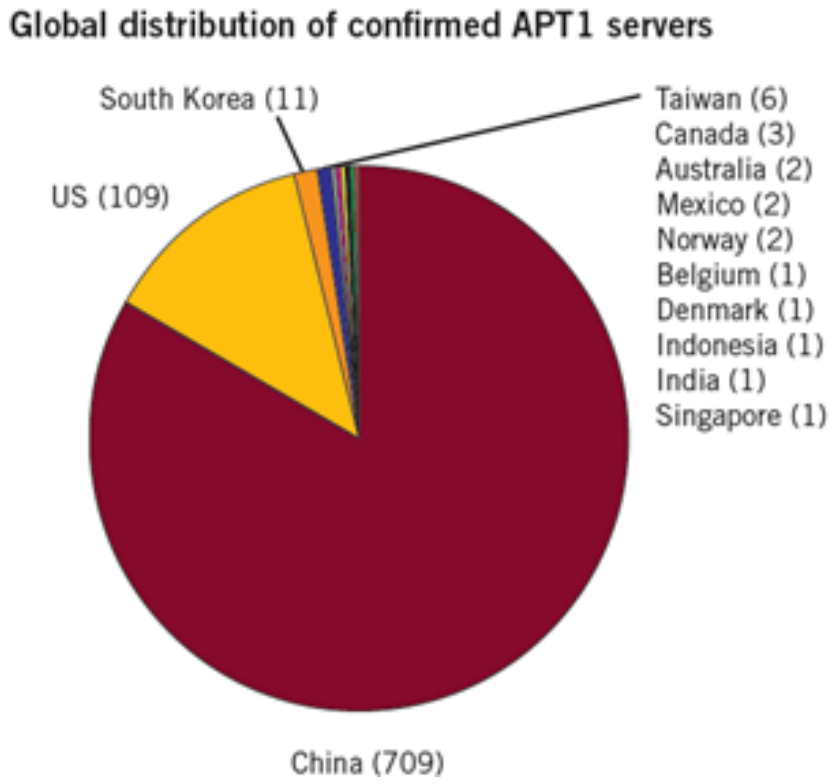

Figure 4: Global Distribution of APT1 Servers (Source: Mandiant APT1 Report)

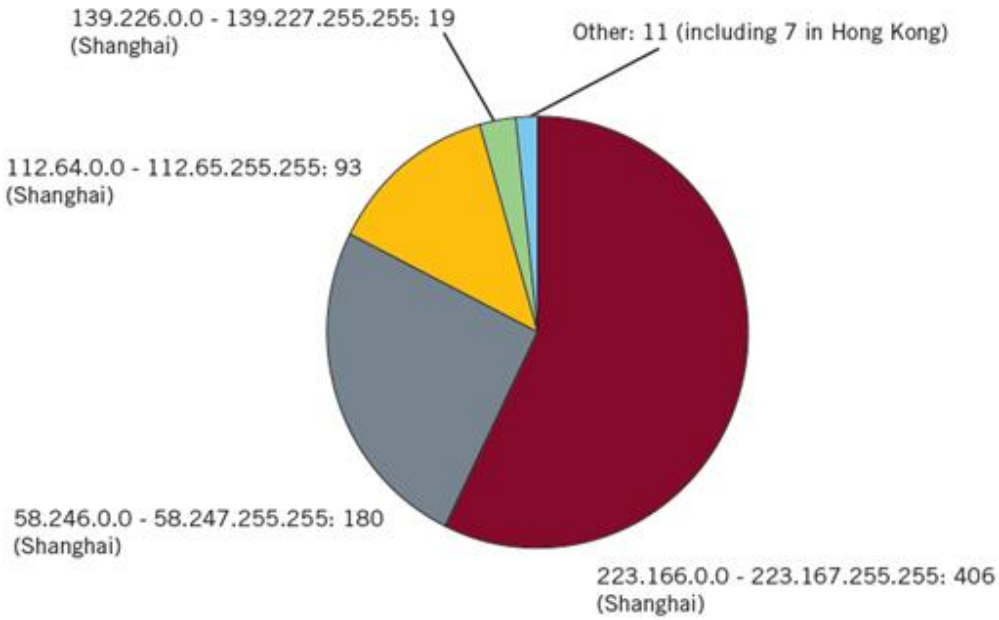

Figure 5APT1 Server's Distribution in China (Source: Mandiant APT1 Report)

APT1 Attack Methodology:

Typical APT1 Attack begins by sending a Spear Phishing E-Mail to the victim. These Emails seem to have official language and themes (suggesting their authenticity) and carry malicious attachment, For Example, an APT1 backdoor that appears to have a pdf extension and icon, which is actually 119 spaces after '.pdf' followed by an '.exe'. When the unsuspecting victim opens the attachment, the backdoor does its job and gives control to the APT1 actor.

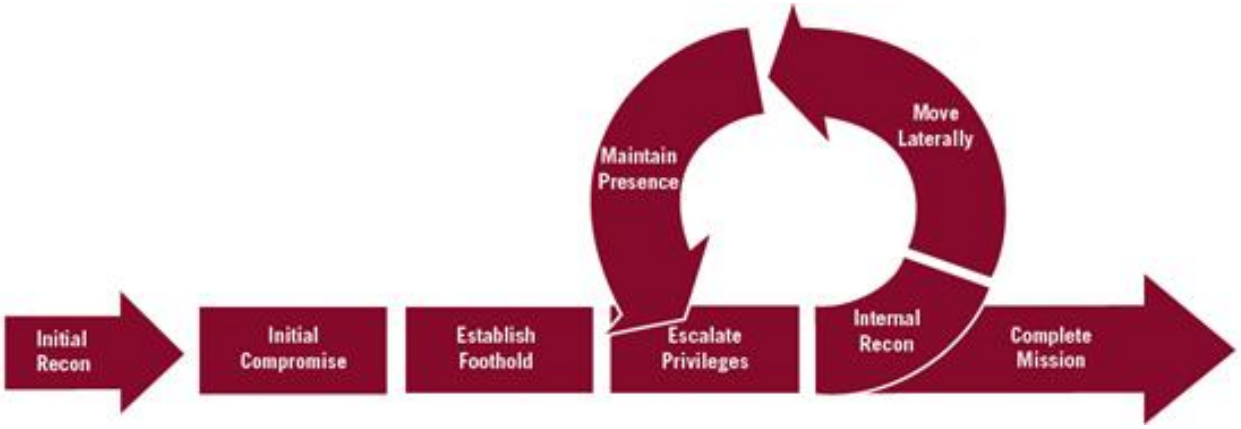

Figure 6: APT1 Attack Lifecycle (Source: Mandiant APT1 Report)

As the main purpose of APT1 actors is to steal confidential documents, once access is obtained to victim's systems, documents are gathered, zipped in a 'rar' file and password-protected. Then this rar archive is sent to the APT1 Actor.

Captured attacker session Video

This video given by Mandiant shows an active attacker's session:

- The Hacker makes an operational Email account on Gmail (named as 'dota'). First he tries to fake his location and enters 'USA' but then notices that Google requires a mobile verification before you can create the account. So now he enters his country as 'China' and provides a cell phone number that is located in the Shanghai in China.
- 'dota' then logins to his Email account, this Email account is used for Spear-phishing and generating more Email Accounts.

Installing Command and Control Server

- 'dota' checks a RAT called 'Ghost' on his own system in Shanghai. We can see that this Ghost RAT has a GUI with features like "Keylogger', 'File Manager', 'Screen Capture', 'Webcam Capture' 'Remote Shell' and 'Voice Chat'.
- Another APT Actor uses a web C2 command and control server. This has a command line interface. The APT Actor uses this client to 'list' the incoming connection from a victim computer. And two victim computers check in.
- APT Actor can be seen using the stolen credentials to log into a mail exchange server and lists the Inbox contents which show the message

numbers and the size of the messages.

- APT Actor goes to an FTP Server and downloads 'lightbolt', then uses this tool to steal files from the victim machine. The 'lightbolt' tool stores stolen files to password protected 'rar' archive which is then uploaded to an FTP.

Case Study

China believed to have copied MQ-1 Predator Drone through Cyber Hacking

QinetiQ North America (QQ) is a world leading defense technology and Security Company providing satellites, drones and software services to the U.S. Special Forces deployed in Afghanistan and Middle East.

In 2009, China had almost its complete control over QinetiQ TSG's computers stealing 1.3 million pages of documents and 3.3 million pages of Microsoft Excel containing TSG's code and engineering data. These Documents were believed to be used by chinese to build MQ-1 drone.

Figure 7: MQ-1 Predator Drone

Is China really doing it? Are they admitting it?

China says "We have said repeatedly that such attacks are transnational and anonymous and determining their origins is extremely difficult". So they are firmly denying the accusation.

The approach is indirect. First the hacker would compromise a US server then use that for further attacking. The security people would visit that server and then sit there and trace back the activity. After all this evidence, there's no way for them to deny that but they dare not admit the Cyber Espionage. The thinking may be that 'America is doing that all the time, so let us too'.

The most damning evidence against China, is the 'attacker's infrastructure' from which they launch attacks, 98% of the times they were logging in from that one block in Shanghai and 97% of the times they were using Chinese set of characters in their systems.

News groups like CNN were stopped from trying to take pictures of the building and were chased by Chinese military guards. Finally the footage was confiscated (see Figure 8).

Figure 8: Chinese Military Guards chasing the CNN News Crew around the APT1 building

Skepticism around the Mandiant report

Some Security Researchers are raising eyebrows at this report mainly because there are a lot of ways in which an attacker of this level of sophistication would hide his/her location. So why did they not cover up their tracks better? Some agree that the attacks originated in China but are doubtful of their connection with the Chinese government. The attacker session video released by Mandiant shows the attacker use 'common' attack tools like Ghost RAT that are freely available over the Internet which is in contradiction to the 'Advanced' Persistent threats that we are talking about.

Summary

Such attacks are targeted towards private industries that are not equipped to deal with threats from the cyber resources of a nation. So this is government versus private industries, which is not fair. US President Obama says "America must face the rapidly growly threats from Cyber-attacks. Now such attacks are focused on sabotaging our power grids, our financial institutions and our air traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and economy."

We should all be glad that the Virginia based security firm Mandiant decided to expose one of the most prolific Cyber Espionage activity group and make all the relating evidence public.

This bold activity may be initialized by the PLA but there's definitely a government approval. Now that the reports are public, if the APT1 activity still continues then the government is definitely involved, even the top leaders. There seems to be a clear strategic planning behind this. Chinese's government monitors and censors the Internet. China is focusing on economic espionage, stealing trade secrets and structural property and negotiation strategies and passing these off to their companies to compete with other companies worldwide. This is a Massive Cyber Espionage campaign.

What are they trying to achieve? It may be motivated by political reasons. It may be a kind of security against what USA can do. Chinese information gathering system has been morphed into a new kind of mode that would that would make it very scary in terms of its effect.

Today such attacks are inevitable but if the government is alert and vigilant, such attacks can be nipped in the bud, before a serious security breach takes place. However, a casual attitude towards such advanced threats can have disastrous effects on a country and its people.

We can boast all we want but the Bottom-line is that India is seriously lagging in its cyber defense capabilities and there are a handful of actual motivated and driven computer security professionals in India.

A reason for this can be that no formal education is being provided to students interested in security and these individuals then turn towards "certifications" which are either too theoretical and provide no

'hands-on' knowledge or are too costly for an average Indian student or require a prior minimum years of experience in the security domain. Some of these certifications in India are started by individuals claiming to be "Hackers" themselves which take candidates more towards the 'glam' of Hacking Emails or Passwords rather than developing a mature approach towards security. India desperately needs state sponsored programs that teach computer security at master's level to deserving students who clear a well-designed competitive screening process. Cyber espionage is a growing issue and it has to be dealt head-on.

In India, a higher level of Information Security Awareness is required. Hacking is not just a bunch of kids randomly doing thing for fun and profit. It is now a national strategy. Important thing to note is that while in countries like USA, hacking is considered illegal and immoral, Chinese government is considering it as a necessity. What would Indian Industries do if they face such attacks? Individual companies can never fight with a nation. The Indian government's support is indispensable against such cyber activities. Such Cyber Espionage is a violation of sovereignty. This is not a minor issue and will continue to grow more severe if nothing is done. This isn't a group of Rogue Hackers, this is a unit of PLA (People's Liberation Army of China). We need to get smart with each breach. From knowledge comes power.

On the Web

- http://intelreport.mandiant.com/– Mandiant Intelligence Report
- http://www.youtube.com/watch?v=3d2gyydHwmY – CNN News Crew being chased
- http://www.youtube.com/watch?v=6p7FqSav6Ho - Video Showing an Attacker Session

Pranshu Bajpai
bajpai.pranshu@gmail.com

Pranshu Bajpai is a Computer Security Professional specialized in 'Systems, Network and Web Penetration Testing'. He is completing his Master's in Information Security from the Indian Institute of Information Technology.

Currently he is also working as a Freelance Penetration Tester on a Counter-Hacking Project in a Security Firm in Delhi, India, where his responsibilities include 'Vulnerability Research', 'Exploit kit deployment', 'Maintaining Access' and 'Reporting'. He is an active speaker and author with a passion for Information security.