AN INVESTIGATION INTO CYBER ESPIONAGE:ATTACK ON GOVERNMENT OF INDIA'S COMPUTERS &OFFICE OF DALAI LAMA

By
Sivakumar Kathiresan
Digital Security Group
Cognizant Technology Solutions

OWASP

Agenda

1. Shadows in the cloud
2. Core Methodology
3. Cyber Investigation-Technical
4. Command & Control Servers
5. PLA, Chengdu & Patriotic Hacking

Acknowledgement

This presentation is based on the reports

SHADOWS IN THE CLOUD:2010

Investigating Cyber Espionage

JOINT REPORT:

Information Warfare Monitor

Shadowserver Foundation

&

Tracking Ghostnet

Warning

Readers of this presentation are cautioned not to practice or try any of the techniques, commands and services given in this presentation.

Any such unethical behavior is considered as the violation of Federal State's respective IT Security Laws and could be Impersonated with huge penalties.

Shadows in the Cloud

Shadows in the cloud

- *Shadows in the Cloud* documents a complex ecosystems of cyber espionage that systematically compromised government, business, academic and other computer network systems in India, the Offices of the Dalai Lama, the United Nations, and several other countries.

- The report also contains an analysis of data which were stolen from politically sensitive targets and recovered during the course of the investigation.

Tracking Ghostnet

- Tracking Ghostnet: Investigating a *Cyber Espionage Network* was the product of a ten-month investigation and analysis focused on allegations of Chinese cyber espionage against the Tibetan Community.
- The report documented a wide ranging network of compromised computers, including at least 1,295 spread across 103 countries
- 30 percent are determined to be "high-value" targets
- Including ministries of foreign affairs, embassies, international organizations, news organizations, and a computer located at NATO headquarters.
- These included computers at Indian embassies in Belgium, Serbia, Germany, Italy, Kuwait, the United States, Zimbabwe and the High Commissions of India in Cyprus and the United Kingdom.

Core Methodology

Core Methodology

The core of the methodology employed in the Shadows in the cloud investigation rests at the nexus of

- Technical interrogation (Sinkhole)
- Field investigation
- Data analysis
- And Geopolitical, Contextual research

- No one method alone is capable of providing a comprehensive understanding of malware networks; it is through their combination that a complete picture is derived.

Core Methodology

- A technical analysis of exploits and malware used by attackers alone can provide a great deal of insight into capabilities and targets.

- The command and control servers used by the malware can be enumerated, and can sometimes reveal additional information that can be used to identify those who have been compromised and data that may have been exfiltrated from these targets.

- The wider geopolitical considerations, derived from both field investigations and contextual research addressed the issues such as
  -the timing of the attacks
  -the nature of the exploitation
  -including the use of any social engineering techniques
  -and potentially the identity and motivation of the attackers.

Field Investigation

- While monitoring the network traffic of a local NGO, Common Ground, as part of an Internet security audit, traffic from a local WiFi mesh network, TennorNet was also captured, revealing malicious activity.

- An anomaly was detected when analyzing this traffic: computers in Dharamsala were beaconing or checking in with a command and control server(jdusnemsaz.com/119.84.4.43) located in Chongqing,PRC.

- The location of Chongqing is contextually interesting as it has a high concentration of Triads-well known Asian-based organized criminal networks-who have significant connections to the Chinese government and the Chinese Communist Party(Lam 2009).

Field Investigation

- The triads have extended their traditional criminal activities to include technology-enabled crime such as "computer software piracy and credit card forgery and fraud"

- An investigation revealed that the computer on TennorNet generating the malicious traffic belonged to Mr. Serta Tsultrim, a Tibetan Member of Parliament, editor of the weekly Tibetan language newspaper *Tibet* Express and the director of the Khawa Karpo Tibet Culture Centre.

- Tsultrim is also the coordinator of the Association of Tibetan Journalists(ATJ).

Cyber Investigation-Technical

Technical Investigative Activities

DNS Sinkholing – Through registering expired domain names previously used in cyber espionage attacks as command and control servers, investigators were are able to observe incoming connections from still- compromised computers.

- This allowed to collect information on the methods of the attackers as well as the nature of the victims.

Malware Analysis – Malware samples were collected from a variety of attacks that allowed to

-Determine the exploits the attackers used

-The theme used to lure targets into executing the malware

-The command and control servers used by the attackers.

- Malware samples consisted primarily of the files with the PDF, DOC, PPT and EXR file extensions

SinkHole

- A DNS sinkhole server is a system that is designed to take requests from a botnet or infected systems and record the incoming information
- The sinkhole server is not under the control of the malware authors and can be used to gain an understanding of a botnet's operation.
- There are a few different techniques that are used to sinkhole botnet traffic.
- The easiest method is to simply register an expired domain that was previously used to control victim systems.

Technical Investigative Activities

- **Command and Control Server Topography -** It was possible to map out the command and control infrastructure of the attackers by linking information from the sinkhole, the field investigations and the malware analysis.

- Domain names, URL paths and IP addresses used by the attackers were collected. This allowed the researchers to find links between their research and other command and control servers observed in other attacks in prior research.

- **Data Recovery –** Researchers were able to retrieve documents that had been sent to *drop zones* from victim systems and stolen by the attackers

Sinkhole

From the recovered IP addresses we were able to identify the following entities of interest:

- Honeywell, United States
- New York University, United States
- University of Western Ontario, Canada
- High Commission Of India, United Kingdom
- Vytautas Magnus University, Lithuania
- Kaunas University of technology, Lithuania
- National Informatics Centre, India
- New Delhi Railway station(*railnet.gov.in), India
- Times of India, India
- Petro IT, (reserved123.petroitg.com), India
- Federation of Indian Chambers of Commerce and Industry, India
- Commission for Science and Technology for Sustainable Development in the South, Pakistan

Tor

- In 2007, a computer security Researcher, Dan Egerstad collected data and email login credentials for a variety of embassies around the world by monitoring the traffic exiting from Tor exit nodes, an anonymous communications network.

- He was able to obtain user names and passwords for a variety of email accounts, and recovered data associated with the Dalai Lama's office as well as India's defence Research and Development Organization (Zetter 2007a).

- Tor does not automatically encrypt everything that a user does online. Unless the end-point of a connection is encrypted, the data passing through an exit node in the Tor network will be in plain text.

- Since anyone can operate a Tor exit node, it is possible for a malicious user to intercept the plain text communication passing through it.

Enfal

- on one of the command and control servers, we also discovered that the attackers were using Enfal, a well known Trojan.
- The malware connected to www.indexnews.org and requested the following file paths: /cgi-bin/Owpq4.cgi and /httpdocs/mm/[HOSTNAME]_20090610/Cmwhite.
- We explore the broader connections and significance of use of Enfal

Filename	20090924152410520
MD5	9f0b3d0672425081cb7a988691535cbf
C2	www.indexnews.org

Command and control Infrastructure

- The attacker's command and control infrastructure consists of three interrelated components.
- The first component consists of intermediaries that simply contain links, which can be updated, to command and control servers
- The attackers also used Yahoo! Mail accounts as a command and control component in order to send new malicious binaries to compromised computers.
- On at least one occasion the attackers also used Google pages to host malware. To be clear, the attackers were misusing these systems, not exploiting any vulnerability in these platforms.
- The attackers simply created accounts on these services and used the as a mechanism to updates compromised computers with new command and control server information.

Yahoo1 Mail Inbox

- The next time that a compromised computer checks in with the email account, it then downloads and executes the malicious attachment.

- Upon execution, the compromised computer placed an acknowledgement mail in the Yahoo! Mail Inbox.

The email addresses used by the attackers were:

- zhengwai@yahoo.com
- wwwfoxperter@yahoo.com
- swwwfox@yahoo.in
- ctliliwoy5@yahoo.com
- sonamtenphel@yahoo.com

Command & Control Servers

- As some of the free hosting accounts became unavailable, the attacker's modified blogs on the intermediaries to point to new command and control servers, most often to servers that appear to be the core of the network.
- The core command and control servers reside on domain names that appear to be registered by the attackers themselves and on dedicated servers.

- These control servers are
- **c2etejs.com**
- erneex.com
- idefesvn.com
- **jdusnemsaz.com**
- peose.com
- **indexnews.org**
- **lookbytheway.net**
- microsoftnews.net
- tibetcommunication.com
- intoplink.com
- **indexindian.com**

- In addition it is found servers on free domains provided by co.tv and net.ru

- All of the IP addresses to which the sub-domains of these control servers resolve are in the United States , with the exception of one that is hosted in Germany.

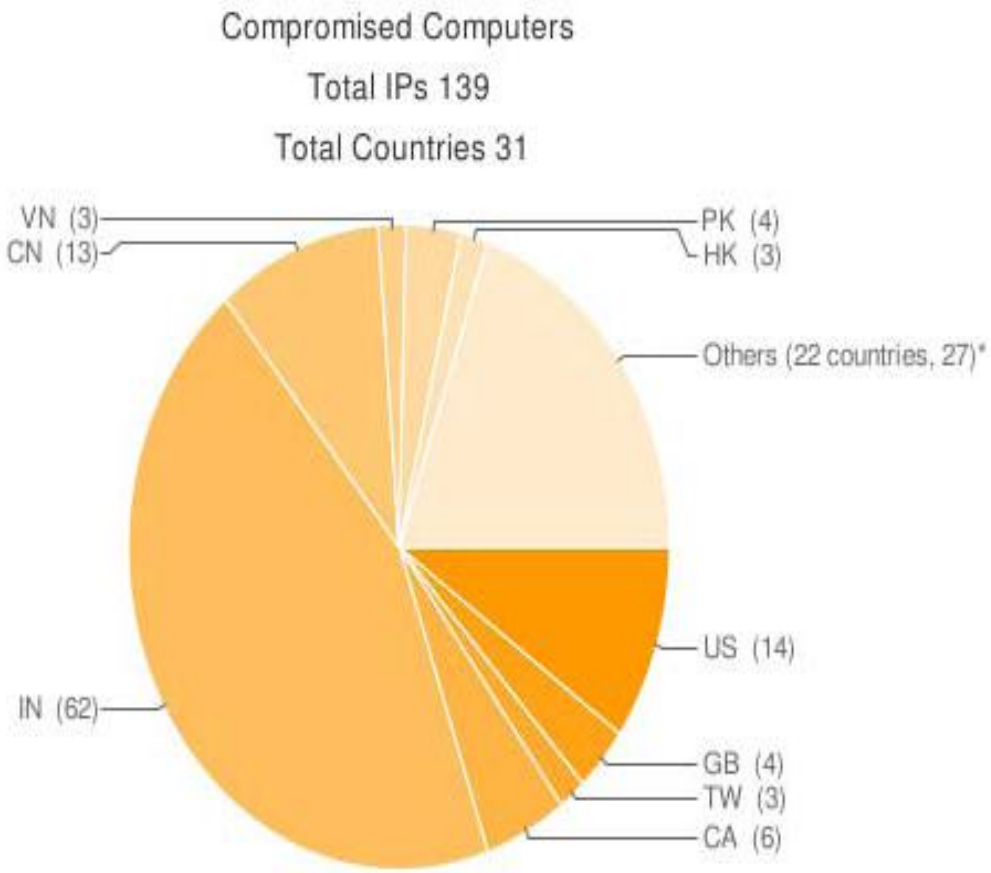
Domain names

- All of these domain names are hosted in the PRC.
- The first group of names (c2etejs.com, erneex.com, idefesvn.com, jdusnemsaz.com, peose.com) were all hosted on the same IP address - 119.84.4.43 - but moved to another IP address – 210.51.7.155 – which is associated with the more well known domain names indexindian.com and tibetcommunication.com.
- The domains indexnews.org and lookbytheway.net are on 188.87.27, microsoftnews.net is on 61.188.87.79 and intoplink.com is on 60.160.182.113.
- The domains indexindian.com, indexnews.org and lookbytheway.net are well known malware domain names associated with more than one instance of malware.

Location of Compromised Computers in the shadow Network

- While there is considerable geographic diversity, there is a high concentration of compromised computers located in India.
- However, we were only able to indentify two of the compromised entities:
- Embassy of India, United States.
- Embassy of Pakistan, United States

- **Diagram**



Targets

- These documents contain sensitive information taken from a member of the National Security Council Secretariat concerning secret assessments of India's security situation in the states of **Assam, Manipur, Nagaland and Tripura. As well as concerning the Naxalites and Maoists**.

- In addition, they contain confidential information taken from Indian embassies regarding **India's International relations with and assessments of activities in West Africa, Russia/Commonwealth of Independent States and the Middle East**, as well as visa applications, passport office circulars and diplomatic correspondence.

- These compromises and the character of the data exfiltrated extends to non-governmental targets as well.

- Some of the academic and journalists that were compromised were interested in and regularly reporting on **sensitive topics such as Jammu and Kashmir.**

National Security and defence

- The attackers also exfiltrated detailed Personal information regarding a member of the Directorate General of Military Intelligence.

Recovered documents and presentations relating to the following projects:

- Pechora Missile System-an anti-aircraft surface-to –air missile system(Russia).

- Iron Dome Missile System-a mobile missile defence system Project Shakti-an artillery combat command and control system.

- Documents relating to network centricity (and network-centric warfare had been exfiltrated, along with documents detailing plans for intelligence fusion and technologies for monitoring and analysing network data (Defence Research and Development Organisation 2009).

Affected Institutions

- National Security Council Secretariat, India
- Diplomatic Missions, India
- Military Engineer Services, India
- Military Personnel, India
- Military Educational Institutions, India
- Institute for defence Studies and Analyses, India
- defence-Oriented Publications, India
- Corporations, India
- Maritime, India
- United Nations

PLA, Chengdu & Patriotic Hacking

Two key pieces of Information

- The first is an email address used in a document in the attacker's possession that provided steps on how attackers could use Yahoo! Mail as a command and control server.
- The second is the IP addresses used by the attackers to send emails from Yahoo! Mail accounts used as command and control servers.
- Email addresses used by the attackers have proven to provide critical clues in past investigations
- *The Dark Visitor* – a blog that researches Chinese hacking activities – investigated one of the email addresses that was to register the domain names the attackers utilized as command and control servers.
- While these were not *GhostNet* domain names, one of them is the same as one used by the attackers in this investigation: **lookbytheway.net**

PLA

- The infrastructure of this particular network is tied to individuals in Chengdu, Sichuan.
- At least one of these individuals has to ties to the underground hacking community in the PRC and to the University of Electronic Science and Technology of China in Chengdu.
- Interestingly, when the Honker Union of China, one of the largest hacking groups in the PRC, was re-established in 2005,its new leader was a student at he University of Electronic Science and Technology in Chengdu.

PLA & Chengdu

- Chengdu is also the location of one of the People's Liberation Army(PLA)'s technical reconnaissance bureaus tasked with signals intelligence collection.

- While it would be disingenuous to ignore these correlations entirely, they are loose at best and certainly do not meet the requirements of determining motivation and attribution.

- However, the links between the command and control infrastructure and individuals in the PRC provide a variety of scenarios that point toward attribution.

Conclusion

- The report analyzes the malware ecosystem employed by the *Shadows'* attackers, which leveraged multiple redundant cloud computing systems, social networking platforms, and free web hosting services in order to maintain persistent control while operating core servers located in the People's Republic of China(PRC).
- Although the identity and motivation of the attackers remain unknown, the report is able to determine the location (Chengdu, PRC) as well as some of the associations of the attackers through circumstantial evidence.
- Although there was circumstantial evidence pointing to elements within the People's Republic of China, there investigation concluded that there was not enough evidence to implicate the Chinese government itself and attribution behind *GhostNet* remains a mystery.
- Governments around the world are engaged in a rapid race to militarize cyber space, to develop tools and methods to fight and win wars in this domain. This arms race creates an opportunity structure ripe for crime and espionage to flourish. In the absence of norms, principles and rules of mutual restraint at a global level, a vacuum exists for subterranean exploits to fill.

Thank you

? Pls