JR02-2009

Tracking *GhostNet*:

Investigating a *Cyber Espionage* Network

Information Warfare Monitor

March 29, 2009

TheSecDevGroup

http://www.infowar-monitor.net/ghostnet
http://www.tracking-ghost.net

University of Toronto
Munk Centre
For International Studies
At Trinity College

March 29, 2009

Foreword

Cyber espionage is an issue whose time has come. In this second report from the Information Warfare Monitor, we lay out the findings of a 10-month investigation of alleged Chinese cyber spying against Tibetan institutions.

The investigation, consisting of fieldwork, technical scouting, and laboratory analysis, discovered a lot more.

The investigation ultimately uncovered a network of over 1,295 infected hosts in 103 countries. Up to 30% of the infected hosts are considered high-value targets and include computers located at ministries of foreign affairs, embassies, international organizations, news media, and NGOs. The Tibetan computer systems we manually investigated, and from which our investigations began, were conclusively compromised by multiple infections that gave attackers unprecedented access to potentially sensitive information.

But the study clearly raises more questions than it answers.

From the evidence at hand, it is not clear whether the attacker(s) really knew what they had penetrated, or if the information was ever exploited for commercial or intelligence value.

Some may conclude that what we lay out here points definitively to China as the culprit. Certainly Chinese cyber-espionage is a major global concern. Chinese authorities have made it clear that they consider cyberspace a strategic domain, one which helps redress the military imbalance between China and the rest of the world (particularly the United States). They have correctly identified cyberspace as the strategic fulcrum upon which U.S. military and economic dominance depends.

But attributing all Chinese malware to deliberate or targeted intelligence gathering operations by the Chinese state is wrong and misleading. Numbers can tell a different story. China is presently the world's largest Internet population. The sheer number of young digital natives online can more than account for the increase in Chinese malware. With more creative people using computers, it's expected that China (and Chinese individuals) will account for a larger proportion of cybercrime.

Likewise, the threshold for engaging in cyber espionage is falling. Cybercrime kits are now available online, and their use is clearly on the rise, in some cases by organized crime and other private actors. Socially engineered malware is the most common and potent; it introduces Trojans onto a system, and then exploits social contacts and files to propagate infections further.

Furthermore, the Internet was never built with security in mind. As institutions ranging from governments through to businesses and individuals depend on 24-hour Internet connectivity, the opportunities for exploiting these systems increases.

This report serves as a wake-up call. At the very least, a large percentage of high-value targets compromised by this network demonstrate the relative ease with which a technically unsophisticated approach can quickly be harnessed to create a very effective spynet…These are major disruptive capabilities that the professional information security community, as well as policymakers, need to come to terms with rapidly.

These are major disruptive capabilities that the professional information security community, as well as policymakers, need to come to terms with rapidly.

Ron Deibert, Director, the Citizen Lab,
Munk Centre for International Studies,
University of Toronto.

Rafal Rohozinski, Principal and CEO,
The SecDev Group,
Ottawa, Canada.

Acknowledgements

This investigation was prepared by a dedicated team of professionals.

Greg Walton conducted and coordinated the primary field-based research in India, Tibetan Missions abroad, and Europe. Greg is a SecDev Group associate and editor of the Information Warfare Monitor website. He is currently a SecDev Fellow at the Citizen Lab. The Indian portion of the field work benefited from the expertise of Dr. Shishir Nagaraja, Security Laboratory, Cambridge University. Dr. Nagaraga visited Dharamsala for a period of five days in September to assist on aspects of the technical data collection.[1]

The technical scouting and computer network interrogation was carried out by Nart Villenueve. Nart is the CTO of Psiphon Inc, and the Psiphon Fellow at the Citizen Lab. His investigations included the discovery and exploration of the *GhostNet* control servers. He led the data analysis research, which included log files gathered in the field, as well as data obtained through technical scouting of the *GhostNet* control servers.

This report represents a collective effort. The drafting team consisted of the following individuals (listed in alphabetical order). Ronald Deibert (Citizen Lab), Arnav Manchanda (SecDev Group), Rafal Rohozinski (SecDev Group and Psiphon Inc.), Nart Villeneuve (Psiphon Fellow, Citizen Lab) and Greg Walton (SecDev Fellow, Citizen Lab). Layout and design was led by Jane Gowan (Psiphon Inc. and Citizen Lab). Belinda Bruce (Blurb Media) and James Tay (Citizen Lab), provided additional support to the team.

Countless others also contributed to the research effort. This includes individuals in India and Tibet, who for security reasons we cannot name. We are also grateful to the Private Office of his Holiness the Dalai Lama, the Tibetan Government-in-Exile, the missions of Tibet in London, Brussels, and New York, and Drewla (a Tibetan NGO).

---

1 Aspects of the research carried out by Dr. Nagaraga focusing on socially engineered malware are published in a separate study. See, *The snooping dragon: social-malware surveillance of the Tibetan movement*, Shishir Nagaraja, Ross Anderson, Cambridge University Computer Laboratory Technical Report, Mar 29 2009

Summary

Trojan horse programmes and other associated malware are often cited as vectors for conducting sophisticated computer-based espionage. Allegations of cyber espionage (computer network exploitation) are increasingly common, but there are few case studies in the unclassified realm that expose the inner workings of such networks.

This study reveals the existence and operational reach of a malware-based cyber espionage network that we call *GhostNet*.

Between June 2008 and March 2009 the Information Warfare Monitor conducted an extensive and exhaustive two-phase investigation focused on allegations of Chinese cyber espionage against the Tibetan community.

We conducted field-based investigations in India, Europe and North America. In India we worked directly with affected Tibetan organizations, including the Private Office of the Dalai Lama, the Tibetan Government-in-Exile, and several Tibetan NGOs. In Europe and North America we worked with Tibetan missions in London, Brussels, and New York. The fieldwork generated extensive data that allowed us to examine Tibetan information security practices, as well as capture *real-time* evidence of malware that had penetrated Tibetan computer systems.

During the second phase of our investigation, the data was analyzed, and led to the discovery of insecure, web-based interfaces to four control servers. These interfaces allow attacker(s) to send instructions to, and receive data from, compromised computers. Our research team successfully scouted these servers, revealing a wide-ranging network of compromised computers. This extensive network consists of at least 1,295 infected computers in 103 countries.

Significantly, close to 30% of the infected computers can be considered high-value and include the ministries of foreign affairs of Iran, Bangladesh, Latvia, Indonesia, Philippines, Brunei, Barbados and Bhutan; embassies of India, South Korea, Indonesia, Romania, Cyprus, Malta, Thailand, Taiwan, Portugal, Germany and Pakistan; the ASEAN (Association of Southeast Asian Nations) Secretariat, SAARC (South Asian Association for Regional Cooperation), and the Asian Development Bank; news organizations; and an unclassified computer located at NATO headquarters.

The *GhostNet* system directs infected computers to download a Trojan known as *gh0st RAT* that allows attackers to gain complete, *real-time* control. These instances of *gh0st RAT* are consistently controlled from commercial Internet access accounts located on the island of Hainan, People's Republic of China.

Our investigation reveals that *GhostNet* is capable of taking full control of infected computers, including searching and downloading specific files, and covertly operating attached devices, including microphones and web cameras.

The vector for spreading the *GhostNet* infection leverages social means. Contextually relevant emails are sent to specific targets with attached documents that are packed with *exploit code* and Trojan

horse programmes designed to take advantage of vulnerabilities in software installed on the target's computer.

Once compromised, files located on infected computers may be mined for contact information, and used to spread malware through e-mail and document attachments that appear to come from legitimate sources, and contain legitimate documents and messages. It is therefore possible that the large percentage of high value targets identified in our analysis of the *GhostNet* are coincidental, spread by contact between individuals who previously communicated through e-mail.

Nonetheless the existence of the *GhostNet* network is a significant fact in and of itself. At the very least, it demonstrates the ease by which computer-based malware can be used to build a robust, low-cost intelligence capability and infect a network of potentially high-value targets.

Key findings:

- **Documented evidence of a cyber espionage network—*GhostNet*—infecting at least 1,295 computers in 103 countries, of which close to 30% can be considered as high-value diplomatic, political, economic, and military targets.**

- **Documented evidence of *GhostNet* penetration of computer systems containing sensitive and secret information at the private offices of the Dalai Lama and other Tibetan targets.**

- **Documentation and reverse engineering of the *modus operandi* of the *GhostNet* system—including vectors, targeting, delivery mechanisms, data retrieval and control systems—reveals a covert, difficult-to-detect and elaborate cyber-espionage system capable of taking full control of affected systems.**

Introduction

Computer network exploitation represents the leading edge of signals intelligence in the information age. The proliferation of computer systems throughout governments, businesses, and civic organizations represents a boon for would-be cyber spies.

Awareness of cyber vulnerabilities, and even basic information security practices, is in its infancy, and largely absent in most organizations outside of the classified realm. Commercial computer systems, which represent most of the world's installed base, are insecure. This lack of security consciousness is reflective of the infancy of the information age. The Internet was never designed for security and, for the most part, there has been little incentive for software manufacturers to make security a first priority in the design and development of products, many of which are destined for consumer and/or small business use.

These challenges are present in advanced industrial societies, but are amplified many times over in developing countries. Ownership of computers is a relative rarity among many government departments. Where they exist, they often use grey market or pirated software. Resources are lacking to employ properly trained computer professionals, and many staff are barely computer literate. In this context, information security is often a distant priority.

And yet, computers in the hands of individuals or at government offices, ministries, embassies, and civic and non-governmental organizations contain information that can be valuable. Files and e-mails with contact information, lists of meetings and attendees, draft position papers, internal PowerPoint presentations, organizational budgets, and lists of visitors can represent items of strategic value to rivals and enemies. Organizations, like individuals, can be subject to identity theft, leading to potentially serious breaches of security.

Rise of the cyber spies

Little is known of the sophistication of state-based cyber espionage capabilities, such as those of the United States, Israel, and the United Kingdom, all considered leaders in this field. They are assumed to be considerable as the security doctrines of these countries treat cyberspace as a strategic domain equivalent to that of land, air, sea, and space.[2]

Other powers including China have made cyberspace a key pillar of their national security strategies. China is actively developing an operational capacity in cyberspace, correctly identifying it as the domain in which it can achieve strategic parity, if not superiority, over the military establishments of the United States and its allies. Chinese cyber warfare doctrine is well developed, and significant resources have been invested by the People's Liberation Army and security services in developing defensive and offensive capabilities.[3]

---

2 http://www.dod.mil/pubs/foi/ojcs/07-F-2105doc1.pdf ; http://www.afa.org/media/reports/victorycyberspace.pdf

3 http://findarticles.com/p/articles/mi_m0PBZ/is_6_88/ai_n31140190 ; http://www.infowar-monitor.net/modules.php?op=modload&name=Archive&file=index&req=viewarticle&artid=2&page=1

But the most significant actors in cyberspace are not states. The online engagements that accompanied the recent Russia-Georgia conflict in August 2008[4] and Israel's January 2009 offensive in Gaza[5] were carried out by independent attackers. The May 2007 denial of service attacks against Estonia[6] resulted in a single conviction of a Russian living in Estonia. Likewise, previous high-profile investigations of hacking against strategic U.S. targets were never positively attributed to foreign intelligence services[7], and in many cases were the work of individuals.[8]

The contest in the shadows currently underway in cyberspace appears to rely largely on third parties. In numerous instances, including case studies conducted by the Information Warfare Monitor's sister project, the OpenNet Initiative, third party attackers were responsible for triggering national-level cyber events. In Kyrgyzstan (2005)[9], Belarus (2006)[10], during the Russia Georgia war (2008), and Kyrgyzstan (2009), individuals and/or loose coalitions were responsible for publishing target lists and attack tools on semi-private websites. The ensuing "cyclones in cyberspace" were sufficient to precipitate events outside of cyberspace.[11]

International cooperation has for the most part focused on establishing capabilities for counteracting the criminal use of cyberspace, and with good reason. In 2009, the FBI estimated that cybercrime is responsible for over $10 billion worth of losses each year.[12] Cybercrime is a relatively low cost, low threshold activity. Techniques such as phishing and targeted malware are easy to construct, and the chances of prosecution are minimal given a general lack of international coordination.

This is slowly changing as national and international authorities become more aware of the threat. The attacks on Estonia, for example, led to the establishment of NATO's Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia.[13] The International Telecommunication Union has also established its own specialized agency, IMPACT, designed to aid intelligence sharing and tracking of

---

4 http://blog.wired.com/defense/2008/10/government-and.html ; http://www.slate.com/id/2197514

5 http://www.csmonitor.com/2009/0123/p04s03-wome.html

6 http://www.webpronews.com/topnews/2008/01/24/man-convicted-in-estonia-cyber-attack

7 For example, a US government investigation of systematic hacking of Department of Defense networks and defence laboratories dubbed 'Titan Rain' never provided conclusive evidence to substantiate allegations that the hacking was conducted at the behest of the Chinese government. http://www.time.com/time/magazine/article/0,9171,1098961,00.html

8 A good example is the 1998 'Solar Sunrise' investigation. The evidence gathered by US authorities eventually led to the conviction of an Israeli citizen, Ehud Tenebaum, although the involvement of Israeli security services was never proven. http://www.sans.org/resources/idfaq/solar_sunrise.php

9 http://opennet.net/special/kg/

10 http://opennet.net/sites/opennet.net/files/ONI_Belarus_Country_Study.pdf

11 http://www.infowar-monitor.net/modules.php?op=modload&name=News&file=article&sid=2146

12 http://kn.theiet.org/magazine/issues/0903/hacking-goes-pro-0903.cfm

13 http://www.nato.int/docu/update/2008/05-may/e0514a.html

malicious criminal activity in cyberspace.[14] Countries such as the United States, Russia and China have also entered into bilateral agreements with allied countries and partners.

A focus on China

Recent allegations of Chinese cyber espionage largely rely on anecdotal evidence. The most common proof provided by victims of these attacks consists of log files or malware that shows connections being made by infected computers to IP addresses assigned to the People's Republic of China.

This kind of evidence is circumstantial at best. Internet usage statistics suggest that focusing on Chinese instances of information warfare is misleading.[15] With 41% of the world's Internet users located in Asia, China alone accounts for the largest national population of Internet users—some 300 million, nearly one-fifth of the global number of users. Coupled with the rapid growth in Chinese use of the Internet—a 1,200% increase in the period 2000-2008—this would more than account for the rise in instances of Chinese-oriented malware.[16]

At the same time, however, allegations of Chinese hacking and exploitation of private and government computer systems are persistent enough to warrant an evidence-based investigation.

This report provides such an investigation.

Outline of report

This report is divided into **three parts**:

Part one provides a brief introduction to the context and background to this report. We examine past allegations of cyber espionage by China-based actors and the challenge of evidence-based research in this field. Part one concludes with a brief description of the methods used in our two-phase investigation.

Part two provides a detailed account of the conduct of our investigation. The findings of each phase are presented sequentially.

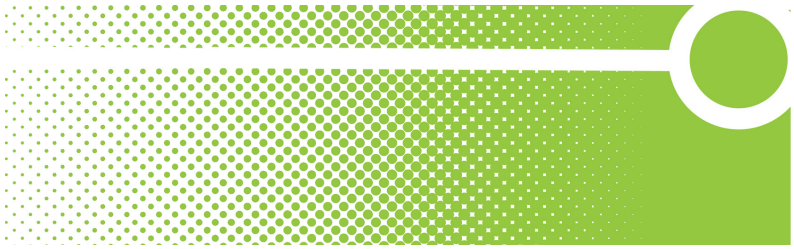
Part three analyses the overall findings of the investigation, suggests alternative explanations and assesses the implications.

---

14 http://www.itu.int/osg/csd/cybersecurity/gca/impact/index.html

15 For global Internet usage statistics please see http://www.internetworldstats.com

16 http://blog.stopbadware.org/2009/03/03/wheres-the-badware



PART ONE:
Context and background

Context and background: Alleged Chinese operations in cyberspace

China has been developing its cyberspace doctrine and capabilities since the late 1990s as part of its military modernization programme. The Chinese doctrine of 'active defence,' which is the belief that China must be ready to respond to aggression immediately, places an emphasis on the development of cyber warfare capabilities.

The Chinese focus on cyber capabilities as part of its strategy of national asymmetric warfare involves deliberately developing capabilities that circumvent U.S. superiority in command-and-control warfare. The strategy recognizes the critical importance of the cyber domain to American military and economic power and the importance of offensive cyber operations to victory in a modern conflict with the United States. Chinese doctrine also emphasizes the contiguity between military and non-military realms.[17]

In recent years, there has been an increase in allegations that China-based hackers are responsible for high-level penetrations of computer systems in Europe, North America and Asia. Attackers originating in China have been accused of infiltrating government computers in the United States, Britain, France, Germany, South Korea, and Taiwan. China-based hackers have been accused of data theft from foreign government computers and commercial and financial institutions. The U.S. Department of Defense reports it is continuously targeted by Chinese attackers, most notably in the series of attacks since 2003 known as 'Titan Rain,' which targeted the Department of Defense and numerous defence companies.[18]

There are also allegations of attacks originating from China directed against non-governmental organizations active in regions where China has a national interest. This includes organizations advocating on the conflict in the Darfur region of Sudan,[19] Tibetan groups active in India, and the Falun Gong. The majority of attacks involve website defacements, denial of service attacks, or virus writing campaigns. Nationalistic and patriotic cyber-activity by Chinese nationals intensifies during crises, such as during Sino-American or Sino-Taiwanese tensions (see below). To date none of these attacks have been traced back to Chinese state authorities or specific individuals, although many have benefited official Chinese policy and interests.

---

17 http://findarticles.com/p/articles/mi_m0PBZ/is_6_88/ai_n31140190 ; http://www.infowar-monitor.net/modules.php?op=modload&name=Archive&file=index&req=viewarticle&artid=2&page=1 ; http://www.heritage.org/Research/asiaandthepacific/upload/bg_2106.pdf

18 http://www.time.com/time/magazine/article/0,9171,1098961,00.html ; http://findarticles.com/p/articles/mi_m0PBZ/is_6_88/ai_n31140190 ; http://www.afa.org/media/reports/victorycyberspace.pdf

19 http://www.insidetech.com/news/articles/1630-mysterious-forces-hack-pro-tibet-save-darfur-sites ; http://www.washingtonpost.com/wp-dyn/content/article/2008/03/20/AR2008032003193.html

Applying the evidence-based approach to cyber attacks: the challenge of attribution

Determining those responsible for cyber attacks, commonly known as the *attribution problem*, is a major challenge. The Internet was never built with security as a priority. The current version of the Internet's address assignment system, IP V4, provides a wealth of loopholes and methods by which a perpetrator can mask his or her real identity and location. Online identities and servers can be cleverly hidden. Packet flows and connections can be masked and redirected through multiple servers. A clever attacker can often hijack a machine belonging to an otherwise innocent organization and use it as a base for launching attacks.

Hand-in-hand with the problem of attribution is the difficulty of identifying motivating factors behind a cyber attack. Many perpetrators of Internet-based attacks and exploits are individuals whose motivation can vary from a simple profit motive through to fear of prosecution or strong emotional feelings, including religious belief and nationalism. Many cyber attacks and exploits which *seem* to benefit states may be the work of third-party actors operating under a variety of motivations. This makes it difficult to separate the motivation of the individual from the potential motives of the party on whose behalf the attacks have occurred, or a prospective client to which the perpetrator is trying to market his or her wares. In either case, the challenge of identifying perpetrators and understanding their motives gives state actors convenient *plausible deniability* and the ability to officially distance themselves from attacks.

Cyber campaigns can also take on a life of their own. Even though a state might 'seed' a particular campaign through tacit encouragement or the absence of sanctions or prosecutions, these campaigns are inherently chaotic and unpredictable in scope and outcome.[20] Phenomena such as spontaneous 'cyber rioting' can surpass the initial purposes of the cyber campaign. Low barriers to entry to this sort of activity enable anyone with a computer and Internet connection to take part in a cyber-attack.[21] For the most part, governments appear to passively benefit from online manifestations of nationalistic and patriotic fervour, although outcomes are inherently unpredictable.[22]

In China, the authorities most likely perceive individual attackers and their online activities as convenient instruments of national power.[23] A favourite target of Chinese hackers is Taiwanese computer systems, especially during times of Sino-Taiwanese tensions, such as elections and

---

20 http://www.yorku.ca/robarts/projects/canada-watch/obama/pdfs/Deibert.pdf

21 http://worldanalysis.net/modules/news/article.php?storyid=343

22 For instance, during the Russia-Georgia conflict in August 2008, tools were made available online for those who wished to participate in the ongoing 'cyber-war' against Georgian websites. http://blog.wired.com/defense/2008/10/government-and.html ; http://www.slate.com/id/2197514

23 http://findarticles.com/p/articles/mi_m0PBZ/is_6_88/ai_n31140190 ; http://fmso.leavenworth.army.mil/documents/Beijings-rising-hackers.pdf

referendums.[24] In April 2001, following the death of a Chinese fighter pilot after a collision with an American spy plane near the Chinese island of Hainan, Chinese hackers began a sustained campaign to target American computer networks. No link was made with elements of the Chinese government.[25]

However, governments cannot always preserve direct control over such activities; groups can maintain their freelance and autonomous status and undertake their own cyber initiatives that may not always attain official sanction or serve state interests.[26]

Targeting Tibet

Accusations of Chinese *cyber war* being waged against the Tibetan community have been commonplace for the past several years. The Chinese government has been accused of orchestrating and encouraging such activity as part of a wider strategy to crack down on dissident groups and subversive activity.[27] Earlier research has traced these attacks against Tibetan groups to IP addresses registered in the People's Republic of China. The attacks used malware hidden in legitimate-looking email messages, infecting unsuspecting users' computers and exploiting the data on it by sending it to control servers.[28]

The identity of the attackers has never been attributed in a conclusive manner to any specific group or individual.[29] The motivation of those behind the attacks, despite conjecture, is also unproven.

In earlier studies, researchers focused on attacks specifically targeting the Tibetan community. But a wide variety of other victims of computer penetrations have reported infections similar to those used against Tibetan organizations, following a similar *modus operandi* and also reporting to control servers usually located in China. These additional targets include the Falun Gong[30], the U.S. Government, and multinational corporations.[31] While reports of these targeted attacks have circulated, the extent to which attackers successfully exploited the affected computers is unknown.

---

24 http://fmso.leavenworth.army.mil/documents/Beijings-rising-hackers.pdf

25 http://news.bbc.co.uk/2/hi/americas/1305755.stm

26 http://fmso.leavenworth.army.mil/documents/Beijings-rising-hackers.pdf

27 http://www.washingtonpost.com/wp-dyn/content/article/2008/03/21/AR2008032102605.html

28 See, http://isc.sans.org/diary.html?storyid=4177 ; http://isc.sans.org/diary.html?storyid=4176 and http://archive.cert.uni-stuttgart.de/isn/2002/09/msg00086.html for background information on these attacks.

29 Attribution for previous penetrations of Tibetan groups has never been publicly attributed and is not available from open sources. Classified studies may reveal a finer grained detail, as many of the attacks are relatively unsophisticated, and given proper assets, could be traced back to specific locations and presumably individuals.

30 Research by Maarten Van Horenbeeck shows that similar attacks have targeted the Falun Gong. http://www.daemon.be/maarten/Crouching_Powerpoint_Hidden_Trojan_24C3.pdf and http://isc.sans.org/presentations/SANSFIRE2008-Is_Troy_Burning_Vanhorenbeeck.pdf

31 See http://www.businessweek.com/print/magazine/content/08_16/b4080032218430.htm

Conduct of the investigation

From June 2008 to March 2009 the Information Warfare Monitor conducted an in-depth investigation of alleged cyber espionage against the Tibetan community. We chose this case study because of the unprecedented access that we were granted to Tibetan institutions through one of our researchers, and persistent allegations that confidential information on secure computers was somehow being compromised. Our lead field investigator had a long history of working with the Tibetan community, and was able to work with the private office of the Dalai Lama, the Tibetan Government-in-Exile, and a number of Tibetan non-governmental organizations.

The investigation consisted of two distinct phases.

Phase 1: Field-based investigations in India, Europe, and North America (June-November 2008)

Field research was carried out in Dharamsala, India, the location of the Tibetan Government-in-Exile. Follow-up research was conducted at Tibetan missions abroad in London, Brussels and New York. During this phase we had unprecedented access to the Tibetan government and other Tibetan organizations. This allowed us to establish a baseline understanding of information security practices at these locations and to design an evidence-based approach to the investigation.

We also conducted extensive on-site interviews with officials in the Tibetan Government-in-Exile, the private office of the Dalai Lama, and Tibetan non-governmental organizations. The interviews focused on the allegations of cyber espionage. We also sought alternative explanations for leakage of confidential documents and information and examined basic information security practices at these locations.

Network monitoring software was installed on various computers so as to collect forensic technical data from affected computer systems, and initial results were analysed *in situ*.[32] This initial analysis confirmed the existence of malware and the transfer of information between infected computers and a number of control servers.[33]

Phase 2: Computer-based scouting, target selection, and data analysis (December 2008-March 2009)

During the second phase of the investigation, researchers based at the Citizen Lab analysed the data collected by the field team.

The data collected in Dharamsala and at Tibetan missions abroad led to the discovery of four control servers and six command servers. These control servers were identified and geo-located from the captured

---

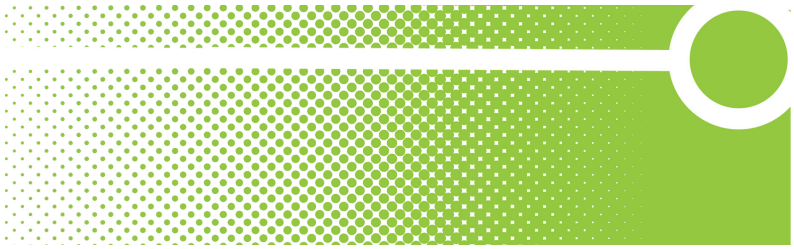
32 A portion of the fieldwork was carried out in conjunction with Dr. Shishir Nagaraja who spent five days in Dharamsala at the request of IWM researchers and assisted in conducting technical tests.

33 A packet capturing program, Wireshark, was installed at each test location. All traffic from each of the affected systems was captured in real-time, and recorded for further analysis. Compromised systems try to connect to control servers in order check-in and report an infection. Once a connection is made, infected computers may receive instructions or additional locations from where they are to download instructions. The Wireshark data is sufficient to analyse these connections, determine the behaviour of the attack vector, and identify the location of control servers.

traffic using a simple IP lookup.[34] The control servers were then probed and web-based control interfaces were identified on four control servers, which allowed us to view and control the network. The system was actively monitored for two weeks, which allowed us to derive an extensive list of infected systems, and to also monitor the systems operator(s) as the operator(s) specifically instructed target computers.

The data collected during both phases was integrated in Palantir, a data visualization and analysis tool. The Palantir platform provides a data fusion and visualization environment that enhances analytical capabilities.

34 We looked up the associated Internet Protocol (IP) address in all five Regional Internet Registries in order to identify the country and network to which the IP address is assigned. We then performed a reverse Domain Name System (DNS) look-up on each IP address. DNS is the system that translates domain names into IP addresses; reverse DNS is a system that translates an IP address into a domain name. This can potentially provide additional information about the entity that has been assigned a particular IP address. If we discovered a domain name, we then looked up its registration in WHOIS, which is a public database of all domain name registrations and provides information about who registered the domain name.



PART TWO:
Tracking *GhostNet*

Phase 1: Field investigation

We conducted our investigation in Dharamsala between July and September 2008. The initial purpose was to gather targeted malware samples from Tibetan NGOs based in the area and to brief the Tibetan Government-in-Exile (TGIE) on the basics of information security. This included raising end-user awareness about social engineering and its policy implications for the secure use of information systems.

The investigator met with the Dalai Lama's representative in Geneva, Tseten Samdup. During the meeting, Samdup inquired about the potential threat to computer security at the Office of His Holiness the Dalai Lama (OHHDL) in light of the targeted malware threat. Samdup requested that the investigator perform a preliminary security review of OHHDL systems, including Dalailama.com and the office computer network. A five day mission was scheduled in early September. Malware was discovered on computers located in the OHHDL.

Following the discovery of malware in the OHHDL, our investigator shifted focus to the campus network of the Tibetan Government-in-Exile. We approached Thubten Samphel, a senior civil servant in the Department for Information and International Relations, and sought permission to run Wireshark on several key computer systems, and to access the firewall logs at the Tibetan Computing Resource Centre. This access was readily granted.

Additional testing was carried out at a Tibetan NGO. This was done at the suggestion of Phuntsok Dorjee, the director of a local NGO, TibTec. Dorjee suggested that we conduct testing and monitoring at the offices of Drewla.[35] As was the case at other sitesthe investigator conducted a series of interviews with the NGO staff.

Targeted malware — previous research

In September 2002, Tibetan groups reported that they were targeted with malware originating from servers in mainland China. They claimed that this was a coordinated attempt to disrupt their operations and *spy* on their computer networks. Similar attacks have occurred since then against a range of Tibetan non-state actors, including exile groups, human rights organizations, trade unions and labour organizers, writers, scholars and intellectuals.

In 2005, a member of our investigating team convened a working group that coordinated the collection and archiving of the malware, including the payloads and associated examples of social engineering employed. Since early 2008, we have analysed every sample available to us, and identified control servers for at least fifty incidents.

During an analysis of attacks which occurred during the 2008 Beijing Olympics we discovered the location of a control server that was later identified as part of the network which infected a computer in the private office of the Dalai Lama.

---

35 The Drewla Initiative Project is an outreach model that seeks new ways to communicate directly with citizens of the People's Republic of China. It relies heavily on the Internet.

We were able to gain access to the command *interface* of this control server and identify the infected computers which reported back to this server. While were are unable to prove exactly how the computer in the Dalai Lama's office became infected, this case demonstrates one of the attack vectors used by the attacker(s) behind the network of infected computers we later uncovered.[36]

The following steps illustrate the attack vector using the malicious document we collected, which was configured to connect to a control server to which we later acquired access. (**See Fig. 1** - p.19)

An email message arrives in the target's inbox carrying the malware in an attachment or web link. The attackers(s)' objective is to get the target to open the attachment or malicious link so that the malicious code can execute. In this case, the attacker(s) sent a carefully crafted email message which was configured to appear as if it was sent from campaigns@freetibet.org with an attached infected Word document named "Translation of Freedom Movement ID Book for Tibetans in Exile.doc" to entice the recipient to open the file.[37] (**See Fig. 2** - p. 20)

Over time, it has been observed that the carrier emails have become more sophisticated in their targeting and content in order to trick their recipients into believing that they are receiving legitimate messages. This is also known as "social engineering." It is common to see legitimate documents recycled for such attacks or the attacker injecting their message into an ongoing group conversation. There are also cases where it appears that content stolen from previously-infected machines was recycled to enhance the appearance of legitimacy.

The targeted user proceeds to opens the attachment or malicious link. Once opened, the infected file or link exploits a vulnerability on the user's machine and installs the malware on the user's computer, along with a seemingly benign file. From the user's perspective, the infected document will often open normally, leaving the user unaware of the infection that just took place.

Only 11 of the 34 anti-virus programs provided by Virus Total[38] recognized the malware embedded in the document. Attackers often use executable packers to obfuscate their malicious code in order to avoid detection by anti-virus software. (**See Fig. 3** - p. 21)

Researchers monitoring the use of socially engineered malware attacks against the Tibetan community have identified over eight different Trojan families in use.[39] Control over some targeted machines is maintained using the Chinese *gh0st RAT* (Remote Access Tool). These Trojans generally allow for near-unrestricted access to the infected systems.

---

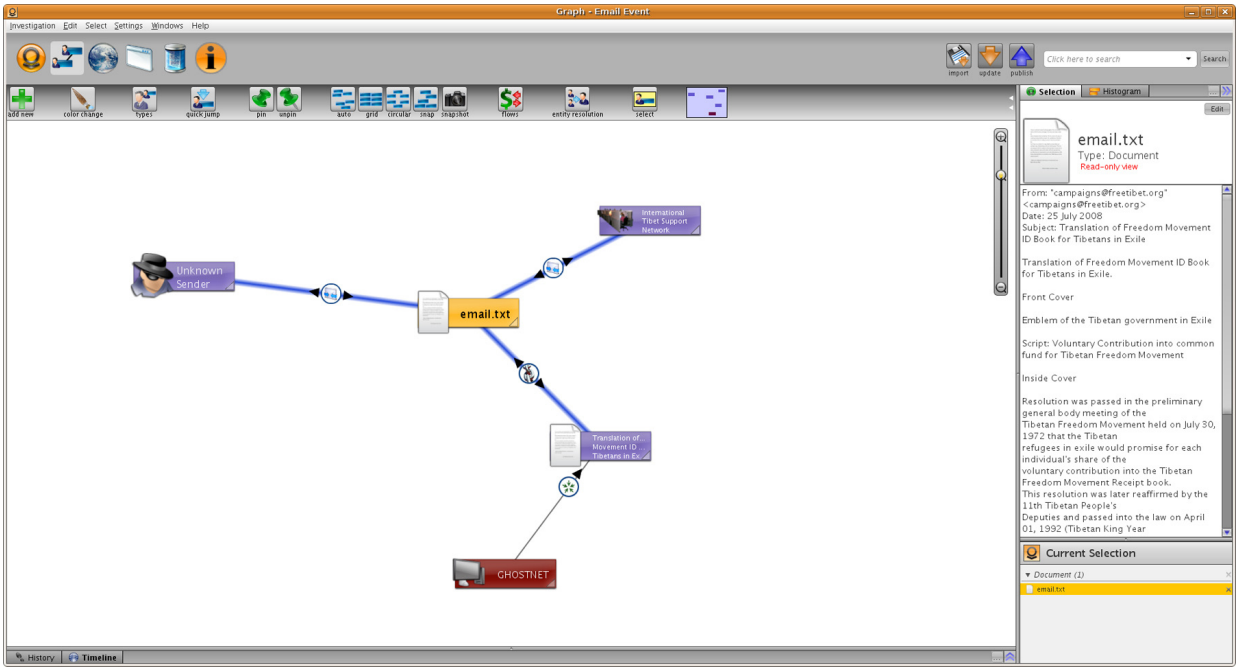
36 A detailed technical investigation of a similar case of a targeted attack which connected to the same control server is available here: [redacted] another investigation of targeted attacks connecting to the same control server is available here: [redacted]

37 For a detailed list of malicious files and control servers see [redacted]

38 VirusTotal.com is a free, web-based service that allows users to upload malicious files that are scanned with 34 leading anti-virus products.

39 http://isc.sans.org/diary.html?storyid=4177

Fig. 1
A "Social Engineering" attack connects to GhostNet.



This Palantir screen capture summarizes the relationships between an "unknown sender" pretending to be "campaigns@freetibet.org", the email sent to the International Tibet Support Network , and the attachment ("Translation of Freedom Movement ID Book for Tibetans in Exile.doc") that contained malware that connected to a *GhostNet* control server.

Fig. 2

A "Socially Engineered" email sent to the International Tibet Support Network.

From: "campaigns@freetibet.org" <campaigns@freetibet.org>
Date: 25 July 2008
Subject: Translation of Freedom Movement ID Book for Tibetans in Exile

Translation of Freedom Movement ID Book for Tibetans in Exile.

Front Cover

Emblem of the Tibetan government in Exile

Script: Voluntary Contribution into common fund for Tibetan Freedom Movement

Inside Cover

Resolution was passed in the preliminary general body meeting of the
Tibetan Freedom Movement held on July 30, 1972 that the Tibetan
refugees in exile would promise for each individual,Äôs share of the
voluntary contribution into the Tibetan Freedom Movement Receipt book.
This resolution was later reaffirmed by the 11th Tibetan People,Äôs
Deputies and passed into the law on April 01, 1992 (Tibetan King Year
2119)

Until the last page of this book is used, the book stands valid until
August 15, 2012

Date: August 16, 2008
Emblem of the Tibetan Government in Exile

Official Signature

Attachment: Translation of Freedom Movement ID Book for Tibetans in Exile.doc

This email was sent on July 25, 2008 by an unknown attacker pretending to be "campaigns@freetibet.org" to the International Tibet Support Network. Attached to the message was a Microsoft Word document named "Translation of Freedom Movement ID Book for Tibetans in Exile.doc" that exploits a vulnerability in Word to install malware on the target's computer system.

Fig. 3
A Virus Total screen capture of a malware infected email attachment.

Antivirus	Version	Last Update	Result
AntiVir	-	-	EXP/Word.Dropper.Gen
Authentium	-	-	CVE-2006-2492
Avast	-	-	MW97:CVE-2006-2492
eTrust-Vet	-	-	W97M/SmartTags!exploit
F-Prot	-	-	CVE-2006-2492
Fortinet	-	-	MSWord/ObjPointer.A!exploit.M20062492
GData	-	-	MW97:CVE-2006-2492
Ikarus	-	-	Virus.MW97.CVE.2006.2492
Microsoft	-	-	Exploit:Win32/Wordjmp.gen
Sophos	-	-	Troj/MalDoc-Fam
Webwasher-Gateway	-	-	Exploit.Word.Dropper.Gen

This is a screen capture from VirusTotal.com, a free, web-based service that allows users to upload malicious files that are scanned with anti-virus products. It shows that only 11 of 34 anti-virus products detected the malicious file ("Translation of Freedom Movement ID Book for Tibetans in Exile.doc").

After infecting the target, the Trojan packed in the Word document performed a DNS look-up to find its control server and then connected to that server. This Trojan attempted to connect to [redacted]. This is one of the control servers that we later scouted and was in the same Trojan family that infected computers in the Dalai Lama's private office.

About 70% of the control servers behind the attacks on Tibetan organizations are located on IP addresses assigned to China. However, servers have also been identified in the United States, Sweden, South Korea and Taiwan. The host names pointing to these servers are quite often configured on dynamic DNS services, such as 3322.org. While these services in and of themselves are not malicious, they are heavily used in these specific attacks.[40]

Information Warfare Monitor field research

In September and October 2008 the Information Warfare Monitor investigated information security practices and alleged cyber espionage activities on the computer systems in various offices related to the work of the Dalai Lama and other Tibetan groups. The offices that we investigated were: the Office of His Holiness the Dalai Lama (OHHDL), based in Dharamsala, India; the Tibetan Government-in-Exile (TGIE); various Offices of Tibet (OOT) in New York City, London, Paris, Brussels, and Geneva; and the Tibetan activist NGO, Drewla. (**See Fig. 4** - p. 23)

Office of His Holiness the Dalai Lama

The OHHDL is the personal office of the Dalai Lama. The OHHDL provides secretarial assistance and is responsible for all matters related to the Dalai Lama and acts on his behalf. It is worth noting that the OHHDL's primary responsibilities include organization of the Dalai Lama's international schedule, handling all diplomatic, governmental and personal correspondence, and acting as the liaison between the Dalai Lama and officials of the Tibetan Government-in-Exile (TGIE) and the Offices of Tibet (OOT) worldwide. Therefore the OHHDL's computer network is continuously transmitting and receiving extremely sensitive data.

While the Office does not have any *secrets*, it is essentially the hub of the Tibetan movement and thus handles strategic, time-sensitive communications. Examples of these communications include scheduling meetings with world leaders, and, since 2002, coordinating the negotiations between the People's Republic of China and Dharamsala.

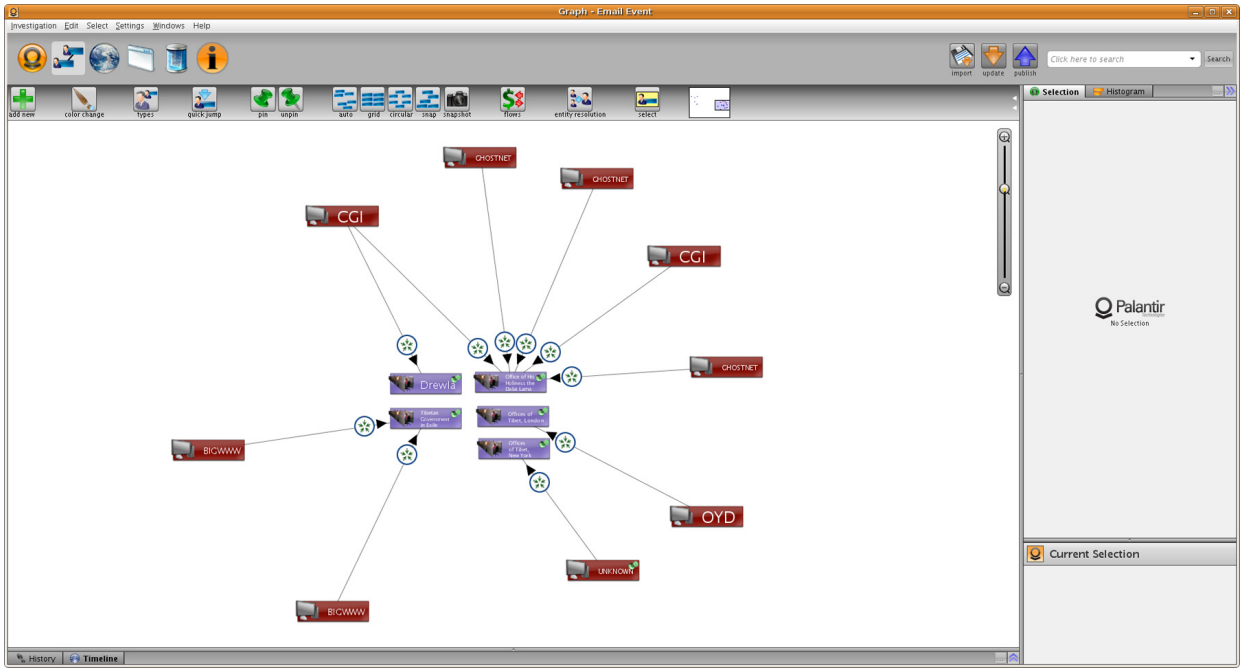
On September 10, 2008, we used Wireshark to capture packets from an OHHDL computer named [redacted] We chose [redacted] from among 23 computers on the OHHDL internal network due to time constraints and consultations with office staff to identify the computers most likely to be infected, such as those operated by relatively inexperienced users vulnerable to social engineering techniques, or those handling particularly sensitive data.

An analysis of the data collected reveals that this computer was compromised by malware that was in interactive communication with identified control servers. The infected computer connected to

---

40 http://www.businessweek.com/print/magazine/content/08_16/b4080032218430.htm

Fig. 4
Field researchers discovered malware at five Tibetan locations.



A Palantir screen capture showing the Tibetan organizations at which we conducted field research and the connections from infected computers at these locations and various control servers located in China. The locations at which we found evidence of infection are: the Office of His Holiness the Dalai Lama, the Tibetan Government-in-Exile, the Offices of Tibet in New York City and London and the Tibetan activist NGO, Drewla.

four different IP addresses, each with a somewhat different method. While there are four groupings of communications between the infected computer and the control servers, they are related such that there appear to be two distinct families of malware. In both cases, the malware uses the protocol for standard web traffic, HTTP, in order make the network activity appear as if it were normal Internet browsing.

The first family of malware used HTTP connections to connect to PHP files.[41] Despite connecting to different IP addresses and requesting different files, both used the same unique key when communicating, indicating that they are part of the same family of malware.

1) The malware made connections to a control server on IP address [redacted] using two host names, [redacted] and [redacted]. The IP address [redacted] is in a range assigned to Hainan-TELECOM [redacted] in China. The malware used HTTP to connect to various PHP files on the control server in order to update its status and receive instructions about where to download commands. The commands are embedded in what appear to be image files (e.g. JPEG).

2) The malware made connections to a control server on IP address [redacted], port 8000. This IP address reverse resolved to [redacted].broad.hk.hi.dynamic.163data.com.cn and is in an IP range assigned to Hainan-TELECOM (HAIFU node adsl dialup ports) in China. The malware used HTTP POST to upload content to the control server.[42]

The investigation carried out in Phase 2 identified the network of control servers used in this particular attack. The control servers we discovered include the control server used in the well-documented instances of social malware used frequently against Tibetan targets during the 2008 Olympics in Beijing.

The second family of malware used HTTP POST to connect to a CGI[43] script to communicate between the infected computer and the control server. While their functions appear to be different, with one malware focusing on reporting and commands and the other on document retrieval, they are likely part of the same family of malware. In addition, the domain names used, www.lookbytheway.net and www.macfeeresponse.org, are registered to the same person, "zhou zhaojun" (losttemp33@hotmail.com).

1) The malware made connections to a control server on IP address 221.5.250.98 using the host name www.lookbytheway.net. The IP address 221.5.250.98 is assigned to CNCGROUP-CQ (CNC Group CHINA169 Chongqing Province Network) in China. The malware on the infected computer used HTTP to connect to a file in an attempt to inform the control server of the infected computer's status and to download commands.

---

41 PHP is a popular scripting language often used in web applications.

42 HTTP POST is a method often used to upload content to a web server.

43 CGI scripts are often written in the Perl programming language.

In one case, the file the infected computer was requesting was not present and the infected computer received a 404 error. However, successful connections were made via HTTP to CGI scripts. The infected computer used HTTP POST to submit data to CGI scripts hosted on the control server.

2) The malware made connections to a control server on 218.241.153.61 using the host name www.macfeeresponse.org. The IP address 218.241.153.61 is assigned to BITNET (Beijing Bitone United Networks) in Beijing, China. The malware on the infected computer used HTTP to connect to a file to inform the control server of the infected computer's status and download commands. In addition, connections were made via HTTP to CGI scripts. The infected computer used HTTP POST to submit data to CGI scripts hosted on the control server. Connections to one CGI script appear to inform the control server of the presence of particular documents, while connections to a second CGI script appear to cause the infected computer to upload documents to the control server using HTTP POST.

Instances of malware that connect to control server locations www.lookbytheway.net and www.macfeeresponse.org have been analysed by security companies.[44] This network extends to a variety of domain names including:

- www.lookbytheway.com – 210.51.7.155
- www.macfeeresponse.com - 210.51.7.155
- www.msnppt.net - 221.5.250.98
- www.msnxy.net - 210.51.7.155
- www.msnyf.com - 221.5.250.98
- www.networkcia.com - 210.51.7.155
- www.indexnews.org - 61.188.87.58
- www.indexindian.com - 210.51.7.155

During the *in situ* investigation at the Dalai Lama's private office we observed several documents being exfiltrated from the computer network and uploaded to www.macfeeresponse.org, including a document containing thousands of email addresses and one detailing and discussing the Dalai Lama's envoy's negotiating position. (**see Fig. 5** - p. 26)

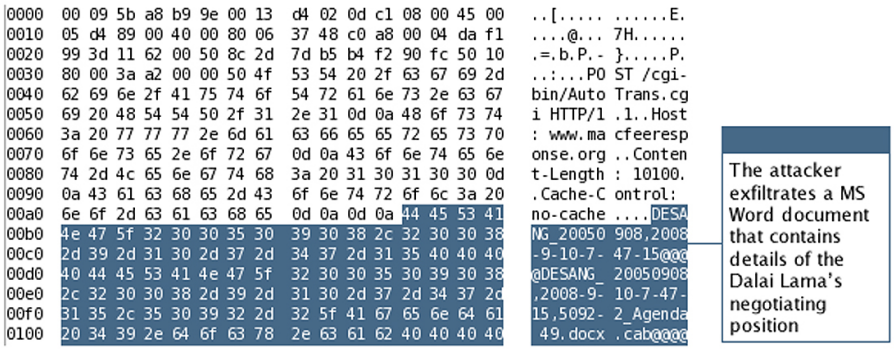
Our investigators did not have access to the stolen documents for reasons of confidentiality. However, we can assume their significance to Sino-Tibetan negotiations. One example is the fact that *GhostNet* penetrated computers of organizations involved in China-TGIE negotiations.[45]

---

44 See, http://www.threatexpert.com/report.aspx?md5=79f7f4695b8878cf1760e8626129ca88 and http://www.threatexpert.com/report.aspx?md5=ea03a7359505e19146994ad77b2a1e46

45 Lodi Gyari is the lead person designated by the Dalai Lama to coordinate negotiations with the Chinese government. Our invesigator interviewed him in December 2008 in Delhi. We briefed him on our ongoing investigation and offered advice on information security while engaged in negotiations in Beijing. Lodi Gyari is also the Executive Chairman of the Board of the International Campaign for Tibet (ICT), an independent Washington-based human rights advocacy group. (Note that our investigation uncovered that seven of ICT's computers were compromised by *GhostNet*).

Fig. 5
Malware retrieving a sensitive document.



This screen capture of the Wireshark network analysis tool shows an infected computer at the Office of His Holiness the Dalai Lama uploading a sensitive document to one of the CGI network's control servers.

Tibetan Government-in-Exile (TGIE)

On September 11, 2008, Wireshark was used to capture packets from a TGIE computer [redacted]. An analysis revealed that this computer was compromised by malware which sent communication to, and received communication from, control servers.

The malware made connections to a control server on 221.10.254.248 using the host name 927.bigwww.com. The IP address 221.10.254.248 is assigned to CNCGROUP-SC (CNC Group CHINA169 Sichuan Province Network) in China. The malware on the infected computer used HTTP to connect to a JPEG file, which was not an image file but instead contains an IP address and port number (124.135.97.21:8005). This IP address, 124.135.97.21, is assigned to CNCGROUP-SD (CNC Group CHINA169 Shandong Province Network) in China.

Offices of Tibet

London

On October 1, 2008 Wireshark was used to capture packets from a computer in the London OOT. An analysis revealed that this computer was compromised by malware which sent communication to, and received communication from, control servers.

The malware made connections to a control server on 58.141.132.66 using the hostname oyd.3322.org on port 4501. The IP address 58.141.132.66 is assigned to NamBu TV in Seoul, South Korea. 3322.org is a Chinese dynamic domain service.

New York

On March 3, 2008, Wireshark was used to capture packets from a computer in the New York OOT. An analysis revealed that this computer was compromised by malware which attempted to send communication to a control server.

The malware attempted to make a connection to what appears to be a control server at 125.108.172.81 but there was not an active server at that location. The IP address 125.108.172.81 is assigned to CHINANET-ZJ-WZ (CHINANET-ZJ Wenzhou node network) in China.

Drewla

Following the discovery of targeted malware on the OHHDL, TGIE and OOT networks, we performed similar analysis on Tibetan NGOs to see if we could identify more infected machines communicating with control servers in China. While we carried out such analysis on a number of NGOs, in this report we focus on Drewla's network.

The Drewla ('connection' in Tibetan) is an online outreach project was set up in 2005 that employs Tibetan youth with Chinese language skills to chat with people in mainland China and in the diaspora, raising awareness about the Tibetan situation, sharing the Dalai Lama's teachings, and supplying information on how to circumvent Chinese government censorship on the Internet.

On September 12, 2008 Wireshark was used to capture packets from a Drewla computer. An analysis revealed that this computer was compromised by malware which sent communication to, and

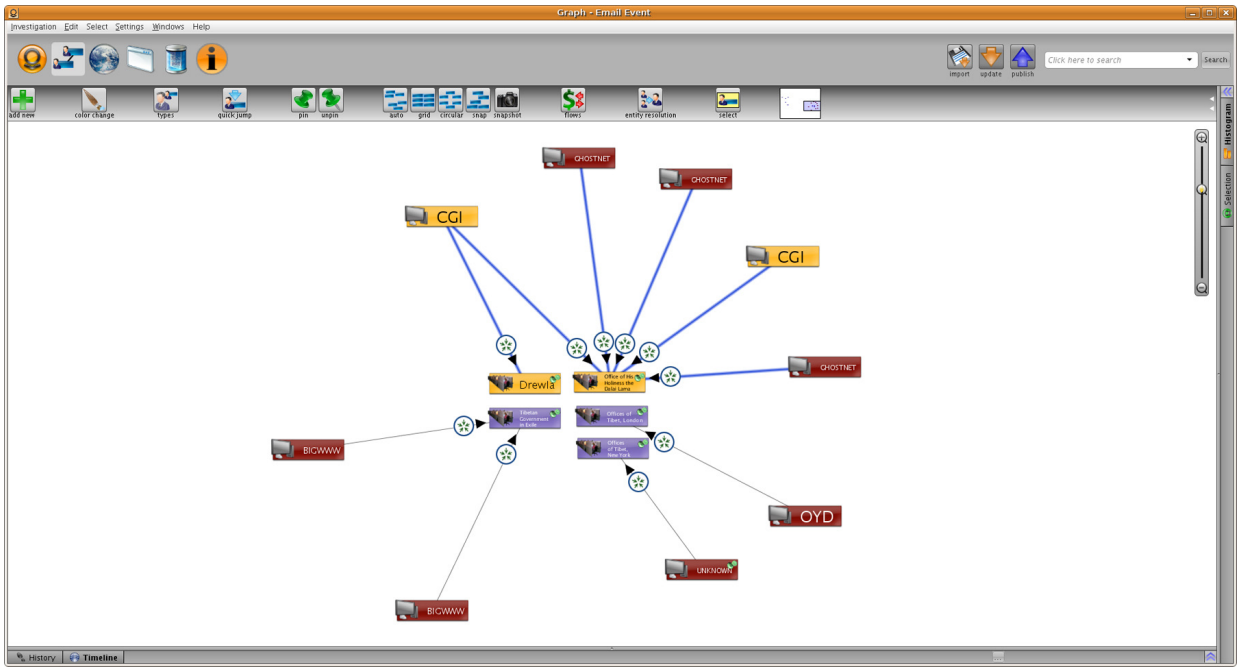
received communication from, control servers.

The malware made connections to a control server on 221.5.250.98 using the host name www.lookbytheway.net. The IP address 221.5.250.98 is assigned to CNCGROUP-CQ (CNC Group CHINA169 Chongqing Province Network) in China. The malware on the infected computer used HTTP to connect to a file in an attempt to inform the control server of the infected computer's status and download commands. The infected computer used HTTP POST to submit data to CGI scripts hosted on the control server. (**see Fig. 6** - p. 29)

Box 1.
Chinese Internet SIGINT in practice

During the course of our research, we were informed of the following incident. A member of Drewla, a young woman, decided to return to her family village in Tibet after working for two years for Drewla. She was arrested at the Nepalese-Tibetan border and taken to a detention facility, where she was held incommunicado for two months. She was interrogated by Chinese intelligence personnel about her employment in Dharamsala. She denied having been politically active and insisted that she had gone to Dharamsala for studies. In response to this, the intelligence officers pulled out a dossier on her activities and presented her with full transcripts of her Internet chats over the years. They indicated that they were fully aware of, and were monitoring, the Drewla outreach initiative and that her colleagues were not welcome to return to Tibet. They then released her and she returned to her village.

Fig. 6
The OHHDL and Drewla were infected by the same malware.



This Palantir screen capture shows the relationship between an infected computer at the Office of His Holiness the Dalai Lama (OHHDL) and the Tibetan NGO Drewla. Both attempted to connect to the same control server in the CGI network.

Phase 2: Identifying command and control servers

This phase of the investigation focused on the discovery of the command and control servers. We were able to identify and connect to the control servers used by the *GhostNet* by analysing the data from the OHHDL obtained during the field investigations carried out in Phase 1. During this process we were able to find and access web-based administration interfaces on the control server identified from the OHHDL data. These servers contain links to other control servers as well as command servers, and so therefore we were able to enumerate additional command and control servers.

After discovering several instances of malware on these servers, we set up a *honey pot* computer and were able to identify additional malicious servers by monitoring the traffic generated by our infected *honey pot*. Using the attacker(s)' web-based administration interface, we were able to command our *honey pot* computer to download *gh0st RAT*, one of the Trojans used by *GhostNet*. Eventually, our *honey pot* computer established a connection to the attacker(s)' *gh0st RAT* client. The attacker(s) proceeded to execute commands on our *honey pot*. We were able to discover several IP addresses within a DSL range in Hainan Island (PRC) that the attacker(s) used to communicate with computers infected with *gh0st RAT*.

Finally, we were able to map out the methods and capabilities of the *GhostNet* by a triangulated analysis of three sources: 1) data obtained from our collection of socially engineered emails with backdoor attachments, 2) the captured network traffic from Tibetan targets; and, 3) data obtained by gaining access to the command and control interface. (**see Fig. 7** - p. 31)

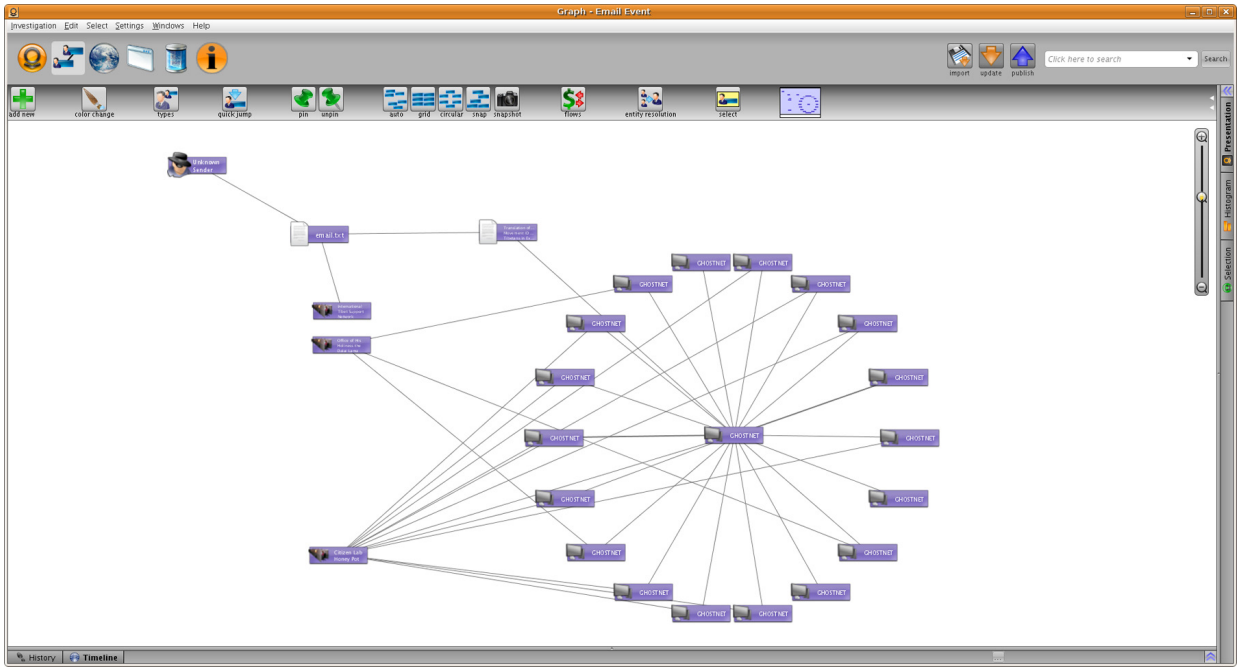
While analysing the data collected from the infected OHHDL computer [redacted], we discovered web-based administration *interfaces* to four control servers. Through some *strategic guessing* concerning file paths and file names, we were able to access web interfaces to multiple control servers. In total, we found 26 instances of the administration interface across the four servers. It remains unclear why the attacker(s) did not secure access to the control interface. Perhaps the attacker(s) concluded that the file paths and file names could not be easily guessed.

The control servers' web interface contains three main components: 1) a listing of all the infected computers that have reported to the control server; 2) an interface to issue commands to the infected computers; and 3) an interface to monitor pending commands to infected computers and their results when completed.

The commands issued to the infected computers direct the infected computer to download files from additional *command servers* under the attacker(s)' control. In some cases, these servers act as control servers themselves; however, some appear to be used exclusively to host malicious files that infected computers are meant to download. The attacker(s) set commands on the control servers that instruct infected computers to download additional remote administration Trojans, such as *gh0st RAT*, in order to take complete real-time control of the infected computers.

Three of the four control servers are located in three different locations in China: Hainan, Guangdong and Sichuan. One of the control servers is located at a web-hosting company in the United States. Five of the six command servers are located in mainland China (Hainan, Guangdong, Sichuan and Jiangsu) and one in Hong Kong.

Fig. 7
The *GhostNet* control servers.



This Palantir screen capture shows the *GhostNet* servers we uncovered and their relationship with the malicious email sent to, 1) the International Tibet Support Network, 2) the infected computer at the Office of His Holiness the Dalai Lama; and, 3) the *honey pot* network set up at the Citizen Lab.

The four control servers are:

- [redacted], Hainan-TELECOM, CN
- [redacted] US
- [redacted] CHINANET-GD, CN
- [redacted] CHINANET-SC, CN

The six control/command servers are:

- [redacted] CHINANET-HI, CN
- [redacted] CUHKNET, HK
- [redacted] CHINANET-GD, CN
- [redacted], CHINANET-SC, CN
- [redacted], CHINANET-JS, CN
- [redacted] CHINANET-SC, CN

The data obtained from WHOIS records concerning domain name registration reveals that most of the domains are traceable to the same individual. However, the attacker(s) could have simply stolen the domains from someone else, or compromised the servers hosting these domains.

Table 1: Domain name registration information

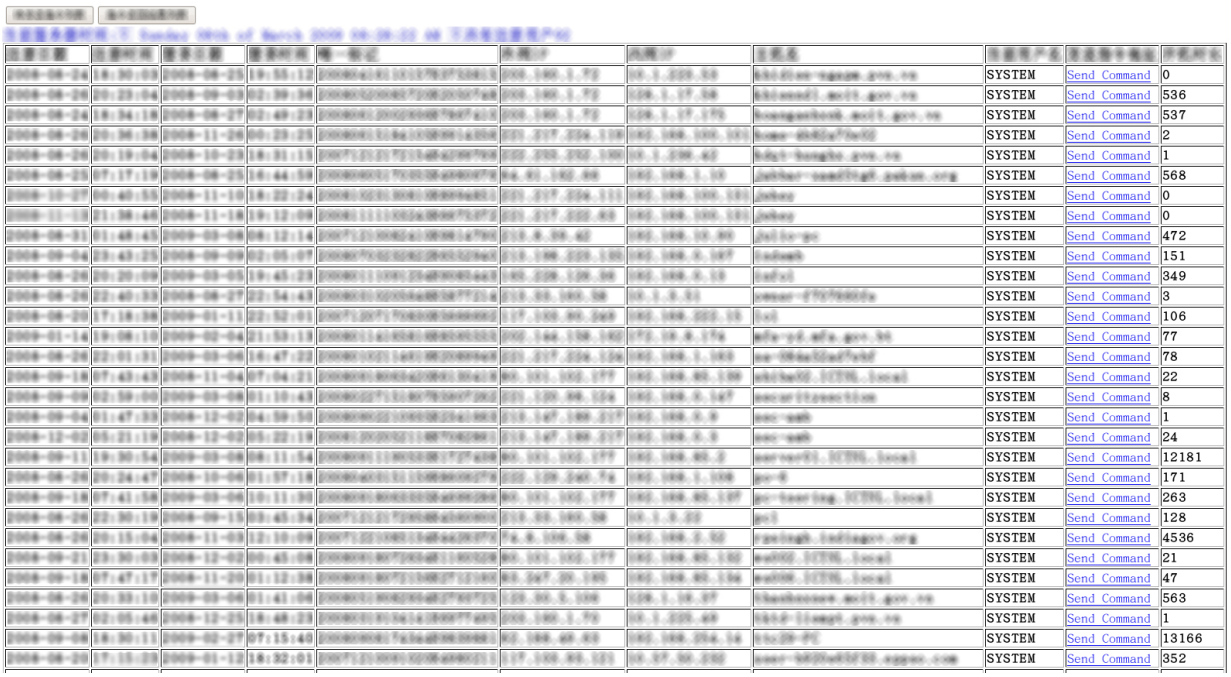
[redacted]	[redacted]	25/04/06
[redacted]	[redacted]	26/11/07
[redacted]	[redacted]	20/06/08
[redacted]	[redacted]	03/09/08

List of infected computers (**see Fig. 8** - p. 33)

The *Server List* interface provides information on each computer infected by the attacker(s)' malware, indicating the name given to the computer (by its owner/operator), its IP address, when it was first infected, when it last *called home* (i.e. the control server), and how many times it has *called home*. Each infected computer is assigned a unique identification number so that the infected computer can be tracked even when its IP address changes. The page also features a link to the *Send Command* interface, through which the attacker(s) sends instructions to the infected

Fig. 8

The *GhostNet* "Server List" interface.



This screen capture of the *GhostNet* interface shows all infected computers that have "checked in" with the control server. It has been obscured to protect the identity of the victims.

computers. There is also a button at the top of the page that links to a *Command Result* page that shows the status of the commands sent to the host and their results.

To corroborate our findings, there was an entry in the *Server List* page of the infected OHHDL computer that we analysed during our field investigations outlined in Part One. It contained the unique ID, the IP address, computer name, and a link to issue commands to the infected computer.

Sending commands

The *Send Command* link provided for each entry yields an interface that allows an attacker(s) to send specific commands to the selected infected computer. In addition to a custom command, the attacker(s) may choose from a menu of commands, which includes options to download binaries that provide additional functionality (such as keystroke logging or remote administration), acquire system information (list computer information, software and documents on the computer), or cause the malware to become dormant. (**See Fig. 9** - p. 35)

Using the *Send Command* interface, the attacker(s) issues instructions to the infected computers to download malicious files that are disguised as standard image files. As mentioned above, the files are most often hosted on additional command servers that appear to be dedicated to hosting these infected files.[46] These command servers contain a variety of files. While the exact function of each file is not known, the file names given to them by the attacker(s) provide some indication of their functionality. There are file names associated with the retrieval of files as well as keystroke logging.

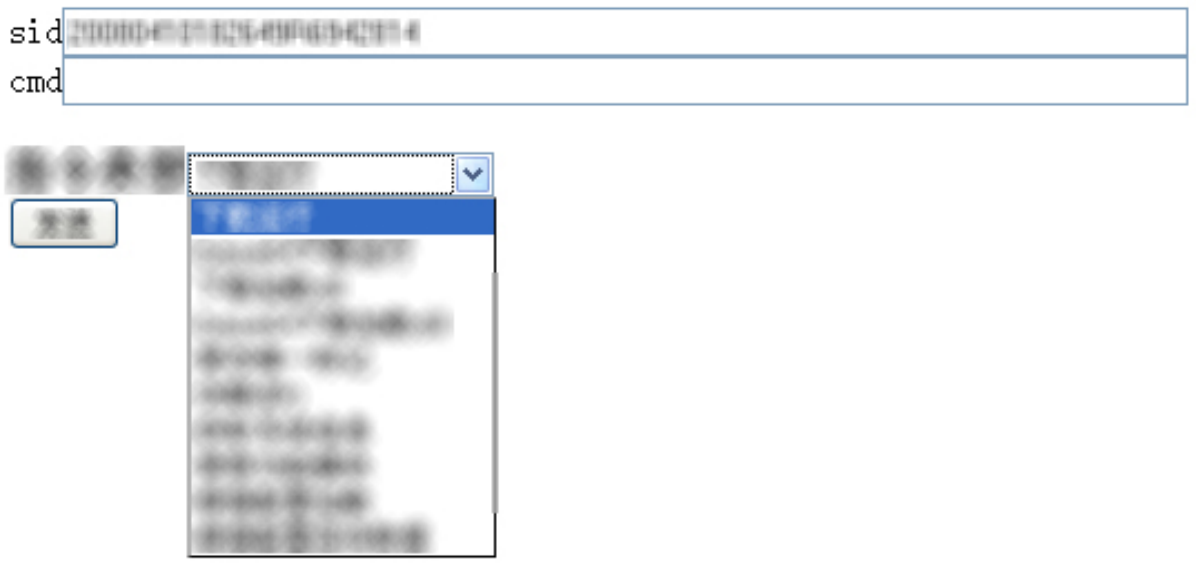
One of the commands available to the attacker(s) instructs infected computers to download the *gh0st RAT* remote administration tool, which gives the attacker(s) full, real-time control of the infected computer. *Gh0st RAT* is an open source Trojan that is widely available online. It was developed by Chinese programmers but has now been translated into English. The program allows an attacker to create an executable file that can be repacked and disguised and used to infect and compromise a target computer. This file can be configured to directly connect to the *gh0st RAT* owner or to a third location, a control server, when it retrieves the current IP address of the *gh0st RAT* owner. (**See Fig. 10** - p. 36)

Once the infected computer connects to the *gh0st RAT* owner, an entry appears in the *Connection* window with some information about the infected computer. The *gh0st RAT* owner may then issue commands to the infected computer. These commands include file manager, screen capture, keylogger, remote shell, system, webcam view, audio capture, as well as the ability to force the infected host to download and execute additional malware, such as a *gh0st RAT* update.

During the course of the investigation, we infected a *honey pot* computer with the attacker(s)' malware. We instructed our infected computer to download the attacker(s)' version of *gh0st RAT* using the malicious network's web-based administration interface. The *gh0st RAT* attempted to connect to several *.broad.hk.hi.dynamic.163data.com.cn IP addresses before finally successfully connecting to [redacted].broad.hk.hi.dynamic.163data.com.cn).

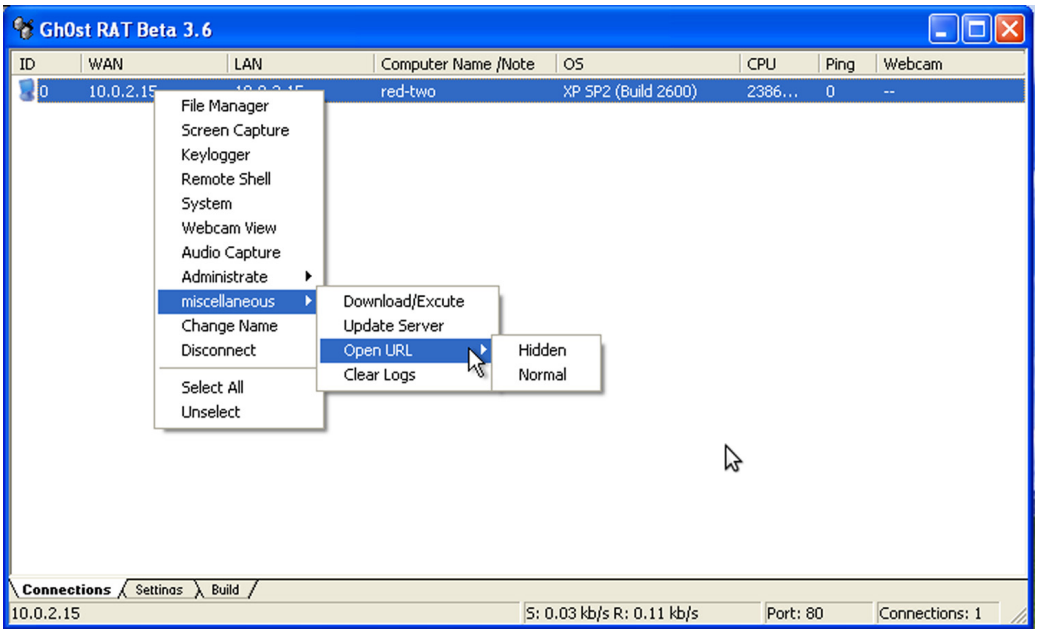
46 In some cases the malicious image files are hosted on the control servers themselves.

Fig. 9
The *GhostNet* "Send Command" interface.



This screen capture of the *GhostNet* interface shows how the attacker(s) can send specific commands to infected computers. It has been obscured to protect the identity of the victims.

Fig. 10
The *ghOst RAT* interface.



This screen capture of the English language version of the *ghOst RAT* software shows the commands that an attacker is able to execute on the compromised computer.

The gh0st RAT tool attempts to connect to IP addresses of a DSL provider in Hainan, China:

- [redacted].broad.hk.hi.dynamic.163data.com.cn
- [redacted].broad.hk.hi.dynamic.163data.com.cn
- [redacted].broad.hk.hi.dynamic.163data.com.cn
- [redacted].broad.hk.hi.dynamic.163data.com.cn
- [redacted].broad.hk.hi.dynamic.163data.com.cn
- [redacted]broad.hk.hi.dynamic.163data.com.cn

After a successful connection, the attacker(s) proceed to issue commands on our infected computer in real-time.

We found similar but unsuccessful connections to the same IP address range from some of the infected computers we analysed and discovered that a rudimentary version of the web-based administration interface contained only one infection from the same IP address range in Hainan. In addition, one of the servers used to host the attacker(s)' malicious files is a Government of Hainan web server located in Hainan, and one of the control server interfaces we gained access to is also located in Hainan. However, one should not rush to judgement concerning the identity of the attacker(s) based on this location. The *gh0st RAT* software can be configured with a proxy server; therefore it is possible that the attacker(s) were using a compromised system as a proxy to hide their true location.

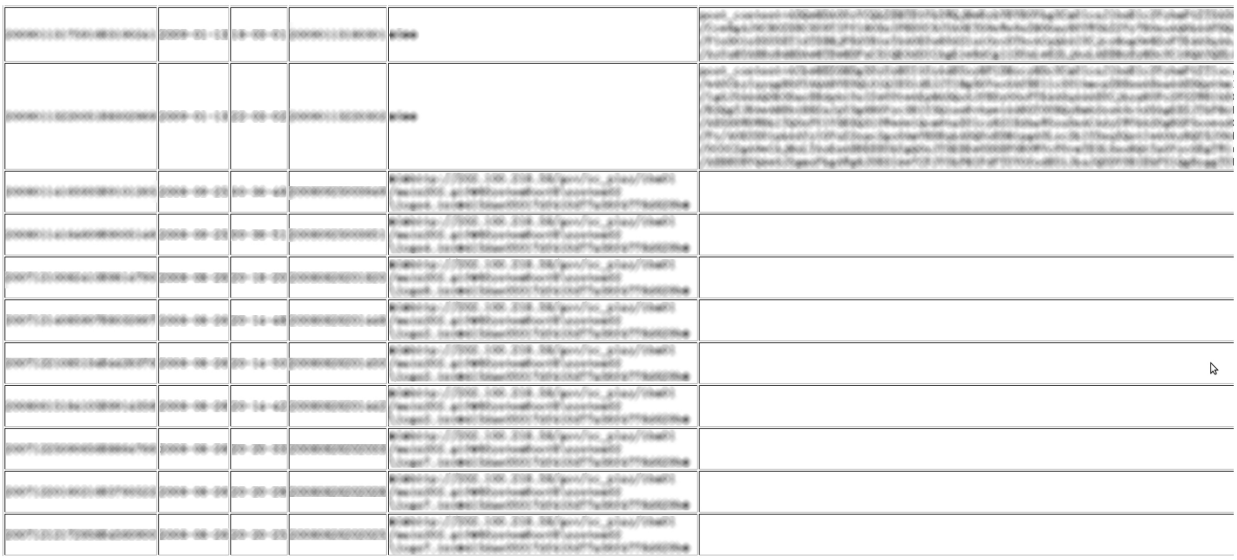
Command results

The *Command Result* page lists the commands issued through the *Send Command* page and the status of those commands. Each entry in this interface shows what command was sent to the infected computer, including the URL to the command server and the command file (the malicious file disguised as an image). Upon the successful completion of a command, the relevant date, time, and result are recorded. (**See Fig. 11** - p. 38)

The *Command Result* page contains a column that displays the content sent back to the control server from the infected computer. The command issued to retrieve this content in the *Send Command* interface is labelled "Acquire System Information." Even though we have been unable to properly decode the content,[47] the plain text values in the binary content indicate that these entries contain information about the infected computer (CPU, memory, operating system, programmes installed) as well as file names of documents on the computer, presumably for later retrieval. This information is likely used to determine which targets the attacker(s) will further exploit and control using remote administration tools such as *gh0st RAT*.

47 The content is base64 encoded and XORed with values we have yet to identify.

Fig. 11
The GhostNet “List Command” interface.



This screen capture of the *GhostNet* interface lists the commands issued to infected computers. It has been obscured to protect the identity of the victims.

Methods and capabilities

The attacker(s) are able to exploit several infection vectors. First, they create web pages that contain "drive by" exploit code that infects the computers of those who visit the page. Second, the attacker(s) have also shown that they engage in *spear phishing* in which contextually relevant emails are sent to targets with PDF and DOC attachments which, when executed, create *back doors* that cause the infected computer to connect to a control server and await further instructions.

With each successful infection the attacker(s) may use any contextually relevant data to further exploit the targeted community and may also impersonate the initial target in order to infect all the targets' contacts. Finally, the targets themselves may infect others by forwarding infected documents to their contacts. In this way, the network of infected computers grows organically.

The first stage of infection focuses on getting targets to execute malicious code. Once infected, the target's computer routinely checks in with a control server in order to receive further instructions. At this stage, the attacker(s) acquires some initial information regarding the identity of the infected computer.

Newer versions of the administration interface contain a direct link to a web service that looks up the relevant WHOIS information about the IP address of the infected computer along with a simple port scan. This version also does a geoIP lookup on the infected computer's IP address and lists the country in which the computer is located, indicating that the attacker(s) has an interest in the geographical location of the infected computers.

The attack may also issue an acquire *system information* command that causes the infected computer to upload its hardware statistics, list of programs installed, list of recent documents, and current network connections. The attacker(s) may use this information to target the infected computer for further exploitation.

The attacker(s) directs the infected computers to download and install a remote administration Trojan. The attacker(s) have demonstrated a preference for *gh0st RAT* but may choose from a variety of Trojans. The attacker(s) simply browses to the "send command" interface and pastes in a link to a version of *gh0st RAT* on a "command" server under his or her control. The next time the infected computer *checks in* to the control server, it will be instructed to download and execute *gh0st RAT*. Upon completion, the infected computer notifies the control server and the result appears in the attacker(s)' web interface.

Once *gh0st RAT* is installed on the target, the infected computer will periodically check a specific location and retrieve the IP address to which it is supposed to connect. When the attacker(s) is not available, he or she will often change this IP to 127.0.0.1 (localhost) so that the amount of potentially suspicious external traffic is limited. When the attacker(s) is ready to receive connections, the IP address is changed to a valid external IP address.

When the attacker(s) turns on *gh0st RAT*, he or she is able to see all the infected machines that have established connections to him or her. The attacker(s) may then execute a wide variety of commands, including file manager, screen capture, keylogger, remote shell, system, webcam view, audio capture, as well as the ability to force the infected host to download and execute additional malware, such as a *gh0st RAT* update. The attacker(s) may also secretly execute programs on the target computer.

Analysis of list of infected computers

A detailed analysis of the list of infected computers revealed an overwhelming number of unique infections in many countries. The same malware that infected computers at the Dalai Lama's office and other Tibetan organizations had a much more extensive set of targets. The list of entities and locations of those targeted was quite varied.

In total, we found 1,295 infected computers located in 103 countries. We found that we were able to confidently—on a scale of low, medium, high—identify 397 of the 1,295 infected computers (26.7%), and labelled each one as a high-value target. We did so because they were either significant to the relationship between China and Tibet, Taiwan or India, or were identified as computers at foreign embassies, diplomatic missions, government ministries, or international organizations.

Of the remaining infected computers, 536 appear to be computers on private broadband Internet providers. The remaining IP addresses do not reverse resolve and available information on these hosts does not allow us to make judgements regarding the identity or purpose of these computers.

Methodology

We compiled a unified and comprehensive list of infected computers from all the control servers, as there was considerable duplication across them. There were several duplicate entries in the list of infected computers—in some cases, the same infected computer was logged multiple times as it was connecting from a different IP address. In other instances, multiple infected computers were assigned different internal IP addresses and had different computer names but shared the same external IP address. This signifies that there were multiple infected computers sharing Internet access. Where possible, we filtered the results by unique computer name, and if no computer name was present, we filtered by unique external IP address.[48] (**See Fig. 12** - p. 41)

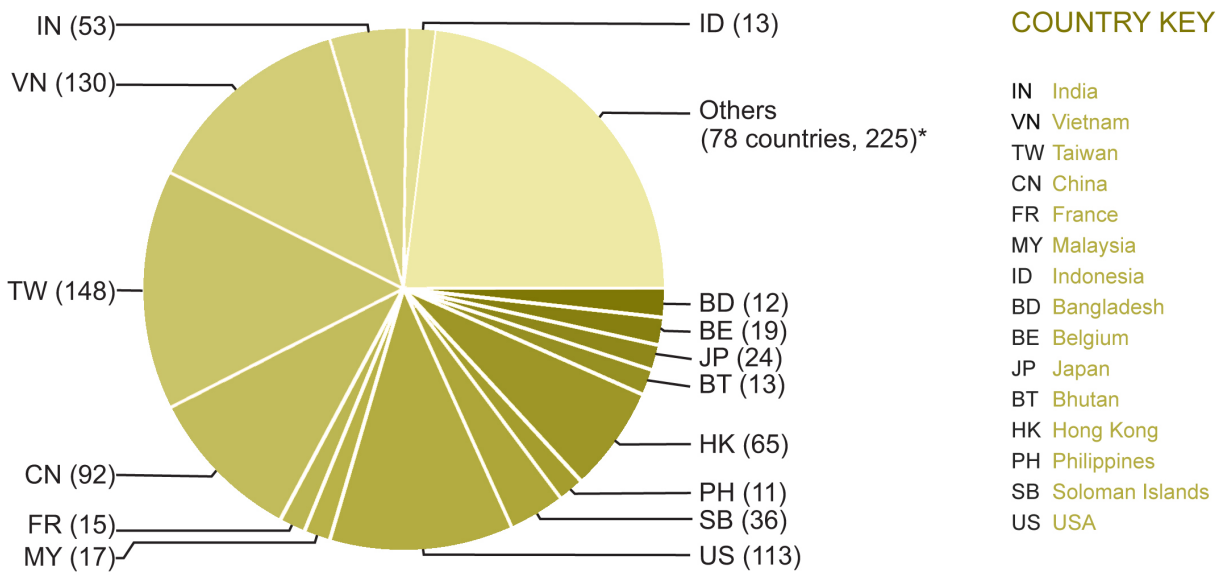
On the surface, the names of the infected computers in the sample are provocative. There are references to ministries of foreign affairs, foreign embassies, and other government entities. Some contains names of officials or their positions/titles. However, we recognize that a computer name can be anything its owner wishes, and may be completely unrelated to the location, function, or owner of that particular computer.

Therefore, in order to be more confident as to the true identity or purpose of the infected computer, we relied on reverse DNS look-ups and each IP address' record from the Regional Internet Registries. Using these two pieces of information we were able to confirm the validity of the identity of several infected computers with a **high (H)** degree of confidence.

In some cases the computer name associated with the infected computer is actually a domain name or an acronym for a recognizable institution or organization. In these cases we classified our identification of the target with either a **medium (M)** or **low (L)** level of confidence. **Medium** confidence refers to instances where we have otherwise identified a related high confidence target,

48 In one case we removed 117 unique IP addresses from Mexico that appeared to belong to the same computer connecting in to the control server from a DSL provider.

Fig. 12
The geographic location of infected hosts.



This graphic illustrates the global reach of the *GhostNet*. There were 1,295 infected computers that reported to the control server. The infections were spread across 103 countries. Taiwan reported the most infections followed by the United States, Vietnam and India.

but for which we rely on the computer name for identification. **Low** confidence refers to instances in which we rely solely on the computer name for identification.

Table 2: Selected infections

Organization	Confidence	Location	Infections
ASEAN	H	ID, MY	3
Asian Development Bank	H	PH, IN	3
Associated Press, UK	H	GB, HK	2
Bureau of International Trade Relations	L	PH	1
CanTV, Venezuela	H	VE	8
Ceger, Portugal	H	PT	1
Consulate General of Malaysia, Hong Kong	H	HK	1
Deloitte & Touche, New York	H	US	1
Department of Commerce, Solomon Islands	L	SB	1
Department of Foreign Affairs, Indonesia	H	ID	3
Department of Foreign Affairs, Philippines	H	PH	1
Department of Science and Technology, Philippines	H	PH	2
Embassy of China, US (see footnote 50)	H	US	1
Embassy of Cyprus, Germany	H	DE	1
Embassy of Germany, Australia	M	AU	1
Embassy of India, Belgium	L	BE	1
Embassy of India, Serbia	L	CS	1
Embassy of India, Germany	H	DE	1
Embassy of India, Italy	H	IT	1
Embassy Of India, Kuwait	H	KW	1
Embassy of India, USA	H	US	7
Embassy of India, Zimbabwe	H	ZA	1
Embassy of Indonesia, China	H	CN	1
Embassy of Malaysia, Cuba	H	CU	1
Embassy of Malaysia, Italy	H	IT	1
Embassy of Malta	L	MT	4
Embassy of Malta, Australia	L	AU	1
Embassy of Malta, Belgium	L	BE	11
Embassy of Malta, Libya	L	LY	1
Embassy of Pakistan, Bahrain	L	BH	1
Embassy of Papua New Guinea, China	L	CN	1
Embassy of Portugal, Finland	H	FI	1
Embassy of Portugal, Germany	H	DE	1
Embassy of The Republic Of China (Taiwan), Swaziland	H	TW	1
Embassy of Romania, Finland	H	FI	1
Embassy of Romania, France	H	FR	1

Table 2: Selected infections (cont'd)

Organization	Confidence	Location	Infections
Embassy of Romania, Norway	H	NO	1
Embassy of Romania, PRC	H	CN	1
Embassy of Thailand, Philippines	H	PH	2
Embassy of the Republic of Korea, China	H	CN	2
Government Integrated Telecommunication Network, Malaysia	L	MY	2
High Commission of India, Cyprus	H	CY	1
High Commission Of India, United Kingdom	H	GB	1
Institute for Information Industry, Taiwan	L	TW	1
International Campaign for Tibet	H	NL	7
International Chamber of Shipping, United Kingdom	L	GB	1
Lanka Education and Research Network, Sri Lanka	L	LK	1
Malta External Trade Corporation Ltd.	H	MT	1
Maritime Police, Solomon Islands	H	SB	1
Ministry of Communications, Brunei	H	BN	1
Ministry of Education, Solomon Islands	H	SB	1
Ministry of Foreign Affairs, Bangladesh	H	BD	4
Ministry of Foreign Affairs, Barbados	M	BB	5
Ministry of Foreign Affairs, Bhutan	L	BT	11
Ministry of Foreign Affairs, Brunei	L	BN	1
Ministry Of Foreign Affairs, Iran	H	IR	1
Ministry of Foreign Affairs, Latvia	H	LV	2
Ministry of Industry and Trade, Vietnam	L	VN	30
Ministry of Labour and Human Resources, Bhutan	H	BT	1
National Informatics Centre, India	L	IN	12
NATO, (SHAPE HQ)	H	NL	1
Net Trade, Taiwan	H	TW	1
New Tang Dynasty Television, United States	L	US	1
Office of the Dalai Lama, India	H	IN	2
Pakistan Mission to The United Nations	L	US, JP	4
Permanent Delegation of Cyprus to the European Union	L	BE	1
Permanent Mission of Cuba to the United Nations	L	US	1
PetroVietnam	L	VN	74
Prime Minister's Office, Laos	H	LA	5
Public Service Division, Solomon Islands	H	SB	1
Russian Federal University Network, Russian Federation	H	RU	1
Software Technology Parks of India, India	L	IN	2
South Asian Association for Regional Cooperation	L	BD, US	5
Students for a Free Tibet, United States	H	US	2
TAITRA, Taiwan	H	TW, NG	79

Table 2: Selected infections (cont'd)

Organization	Confidence	Location	Infections
Taiwan Government Service Network, Taiwan	H	TW	1
Tibetan Government in Exile, India	H	IN, US	4
Trade and Industry Department, Government of Hong Kong	H	HK	1

Infection timeline

The earliest infected computer *called home* to the control server on May 22, 2007. The most recent entry in our sample is March 12, 2009. On average, the amount of time that a host was actively infected was 145 days.[49] While 90 infected computers were only infected for one day, 145 were infected for over 400 days. The longest infection span was 660 days. In total, 422 hosts *checked in* March 1-12, 2009; 373 of these computers were infected in 2008. The data indicates that despite a reduction in new infections, the network continues to be operational. (**See Fig. 13** - p. 45)

There are significant spikes in infection rates in December 2007 and August 2008.

There were 320 infections in December 2007 spread across 56 countries. However, 113 were located within Taiwan and the majority of these infections occurred within a single organization: the Taiwan External Trade Development Council. During this same period, computers at the Embassies of India in Belgium and Zimbabwe were infected as were the Embassies of Indonesia and the Republic of Korea in the People's Republic of China. In addition, computers at the Ministry of Foreign Affairs in Iran were infected as were several computers at the Tibetan Government-in-Exile.

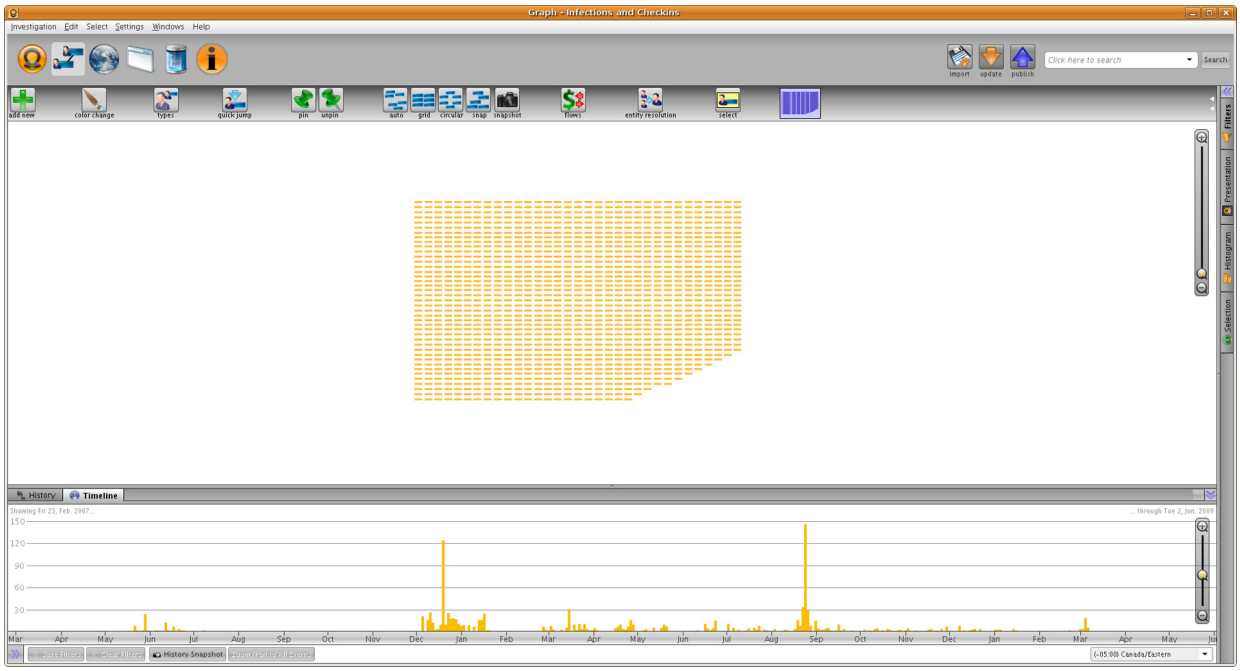
The spike in August 2008 totalled 258 infections spread across 46 countries. The OHHDL computer was infected during one of these spikes in August 2008 (It last checked in to the control server in September 2008). This spike included the Chinese Embassy in the United States,[50] 3 computers at the Embassy of India in the Unites States, and the High Commission of India in the United Kingdom and in Cyprus. It also included the Embassy of Cyprus in Germany, the Embassy of Malaysia in Cuba, the Embassy of Thailand in the Philippines and the Ministry of Industry in Vietnam. Several companies were also compromised, including Net Trade in Taiwan, the New York Office of Deloitte & Touche, and PetroVietnam, the government-owned oil and gas Company.

---

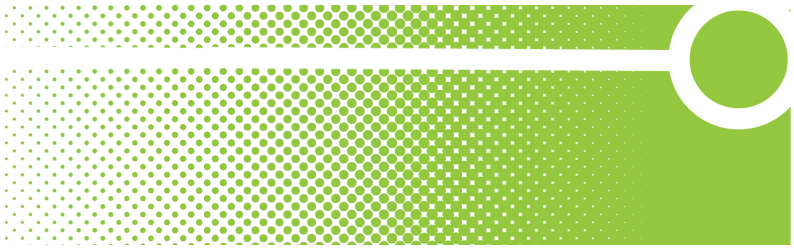
49 The average number of days from the initial infection to the last time an infected computer "checked in" with a control server.

50 It is unclear whether the affected embassy is the Republic of China (Taiwan) or People's Republic of China.

Fig. 13
GhostNet infection timeline.



This screen capture of a timeline generated with Palantir illustrates when and how many computers were infected by the *GhostNet*. It shows that there are significant spikes in infection rates in December 2007 and August 2008.



PART THREE:

Investigating *GhostNet*: Conclusions

The evidence presented in this report—through a combination of field investigations, interviews, technical scouting, data analysis, mining and visualization—paints a disturbing picture.

GhostNet represents a network of compromised computers resident in high-value political, economic, and media locations spread across numerous countries worldwide. At the time of writing, these organizations are almost certainly oblivious to the compromised situation in which they find themselves. The computers of diplomats, military attachés, private assistants, secretaries to Prime Ministers, journalists and others are under the concealed control of unknown assailant(s).

In Dharamsala and elsewhere, we have witnessed machines being profiled and sensitive documents being removed. At our Laboratory, we have analysed our own infected "honey pot" computer and discovered that the capabilities of *GhostNet* are potent and wide ranging. Almost certainly, documents are being removed without the targets' knowledge, keystrokes logged, web cameras are being silently triggered, and audio inputs surreptitiously activated.

This raises the question, how many sensitive activities have been preemptively anticipated by intelligence gathered through this network? How many illegal transactions have been facilitated by information harvested through *GhostNet*? Worst of all, how many people may have been put at risk?

While these questions are compelling, it would be imprudent to read these findings as an indictment, or to attribute to the owners of *GhostNet* motivations and intentions for which there is no evidence.

Alternative explanations

The list of computers controlled by the *GhostNet* is significant, and certainly atypical for a cybercrime network. The size of the network is small, and the concentration of high-value systems is significant.

At the same time, penetrations of this type are not uncommon. Recently, several large-scale spy nets have been discovered, including ones containing lists of affected computers of a magnitude higher than that harvested by *GhostNet*.

This trend is predictable, converging with accumulating incidents of cyber-attacks facilitated by lower entry-thresholds for computer exploitation methods and technologies. The tools we profile in our investigation, though apparently amassed in a complex way to achieve a definite purpose, are not restricted to an exclusive guild of experts with specialized and confidential knowledge.

Today, pirated cyber-crime kits circulate extensively on the Internet and can be downloaded by anyone about as easily as the latest pirated DVD.[51] Cyberspace has empowered individuals and small groups of non-state actors to do many things, including executing sophisticated computer network operations that were previously only the domain of state intelligence agencies. We have entered the era of *do-it-yourself* (DIY) signals intelligence.

---

51 http://ddanchev.blogspot.com/2008/11/zeus-crimeware-kit-gets-carding-layout.html

Attribution

Who is ultimately in control of the *GhostNet* system? While our analysis reveals that numerous politically sensitive and high-value computer systems were compromised, we do not know the motivation or the identity of the attacker(s) or how to accurately characterize this network of infections as a whole. We have not been able to ascertain the type of data that has been obtained by the attacker(s), apart from the basic system information and file listings of the documents located on the target computers. Without this data we are unable to deduce with any certainty what kind of data the attacker(s) were after. There are thus several possibilities for attribution.

The most obvious explanation, and certainly the one in which the circumstantial evidence tilts the strongest, would be that this set of high profile targets has been exploited by the Chinese state for military and strategic-intelligence purposes. Indeed, as described above, many of the high confidence, high-value targets that we identified are clearly linked to Chinese foreign and defence policy, particularly in South and South East Asia. Like radar sweeping around the southern border of China, there is an arc of infected nodes from India, Bhutan, Bangladesh and Vietnam, through Laos, Brunei, Philippines, Hong Kong, and Taiwan. Many of the high profile targets reflect some of China's most vexing foreign and security policy issues, including Tibet and Taiwan. Moreover, the attacker(s)' IP addresses examined here trace back in at least several instances to Hainan Island, home of the Lingshui signals intelligence facility and the Third Technical Department of the People's Liberation Army.[52]

However, we must be cautious to rush to judgement in spite of circumstantial and other evidence, as alternative explanations are certainly possible and charges against a government of this nature are gravely serious. On the other end of the spectrum is the explanation that this is a random set of infected computers that just happens to include high profile targets of strategic significance to China, collected by an individual or group with no political agenda *per se*. Similarly one can postulate that the targets gathered together happened less by concerted effort than by sheer coincidence. Given the groupings of various entities in the infected computer list (by country and organization), internal email communications and sloppy security practices could have led to cross-infection and subsequent listing on the control servers.

Another possible explanation is that there is a single individual or set of individuals (criminal networks, for example) who are targeting these high-value targets for profit. This can be in the form of stealing financial information or critical data that can be sold to clients, be they states or private entities. There are countless examples of large-scale fraud and data theft worldwide and numerous apparent instances of outsourcing to third parties of cyber-attacks and espionage, some of which the Information Warfare Monitor and its related research project, the OpenNet Initiative, have documented. *GhostNet* could very well be a for-profit, non-state venture. Even "patriotic hackers" could be acting on their own volition, or with the tacit approval of their government, as operators of the *GhostNet*.

Finally, it is not inconceivable that this network of infected computers could have been targeted by a state other than China, but operated physically within China (and at least one node in

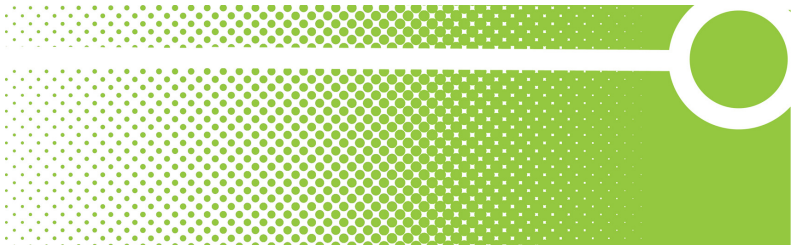
52 http://www.globalsecurity.org/military/world/china/lingshui.htm

the United States) for strategic purposes. Compromised proxy computers on Hainan Island, for example, could have been deployed as staging posts, perhaps in an effort to deliberately mislead observers as to the true operator(s) and purpose of the *GhostNet* system.

The Significance of *GhostNet*

GhostNet is significant, as it does not appear to be a typical cybercrime network. The potential political fallout is enormous. But ultimately, the question of who is behind the *GhostNet* may matter less than the strategic significance of the collection of affected targets. What this study discovered is serious evidence that information security is an item requiring urgent attention at the highest levels. It demonstrates that the subterranean layers of cyberspace, about which most users are unaware, are domains of active reconnaissance, surveillance, and exploitation.

Regardless of who or what is ultimately in control of *GhostNet*, its capabilities of exploitation and the strategic intelligence that can be harvested from it matter most. Indeed, although the Achilles' heel of the *GhostNet* system allowed us to monitor and document its far-reaching network of infiltration, we can safely hypothesize that it is neither the first nor the only one of its kind.



PART FOUR:

About Information Warfare Monitor

About the Information Warfare Monitor

http://infowar-monitor.net/

The Information Warfare Monitor is an advanced research activity tracking the emergence of cyberspace as a strategic domain. We are an independent research effort. Our mission is to build and broaden the evidence base available to scholars, policymakers, and others. We aim to educate and inform.

The Information Warfare Monitor is a public-private venture between two Canadian institutions: The SecDev Group, an operational think tank based in Ottawa (Canada), and the Citizen Lab at the Munk Centre for International Studies, University of Toronto. The Principal Investigators and co-founders of the Information Warfare Monitor are Rafal Rohozinski (The SecDev Group) and Ronald Deibert (Citizen Lab).

The Information Warfare Monitor is supported by The SecDev Group which conducts field-based investigations and data gathering. Our advanced research and analysis facilities are located at the Citizen Lab. IWM is part of the Citizen Lab's network of advanced research projects, which include the OpenNet Initiative and ONI Asia.

The Information Warfare Monitor also benefits from donations from a variety of sponsors including Psiphon Inc, and Palantir Technologies.

The Information Warfare Monitor engages in **three primary activities:**

1. Case Studies. We design and carry out active case study research. These are self-generated activities consistent with our mission.

We employ a rigorous and multidisciplinary approach to all our case studies blending qualitative, technical, and quantitative methods. As a general rule, our investigations consist of at least two components:

> *Field-based investigations*. We engage in qualitative research among affected target audiences and employ techniques that include interviews, long-term *in situ* interaction with our partners, and extensive technical data collection involving system monitoring, network reconnaissance, and interrogation. Our field-based teams are supported by senior analysts and regional specialists, including social scientists, computer security professionals, policy experts, and linguists, who provide additional contextual support and substantive back-up.
>
> *Technical scouting and laboratory analysis.* Data collected in the field is rigorously analysed using a variety of advanced data fusion and visualization methods. Leads developed on the basis of infield activities are pursued through "technical scouting," including computer network investigations, and the resulting data and analysis is shared with our infield teams and partners for verification and for generating additional entry points for follow-on investigations.

2. Open Source Trend Analysis. We collect open-source information from the press and other sources tracking global trends in cyberspace. These are published on our public website.

3. Analytical Workshops and Outreach. We work closely with academia, human rights organizations, and the defense and intelligence community. We publish reports, and occasionally conduct joint workshops. Our work is independent, and not subject to government classification. Our goal is to encourage vigorous debate around critical policy issues. This includes engaging in ethical and legal considerations of information operations, computer network attacks, and computer network exploitation, including the targeted use of Trojans and malware, denial of service attacks, and content filtering.

About The SecDev Group

http://www.secdev.ca

The SecDev Group is a Canadian-based operational consultancy focused on countries and regions at risk from violence and insecurity. We deliver to our clients insights and access to a diverse range of cultures, audiences, challenging environments and *ungoverned spaces*. Our approach combines a field research capability with advanced techniques and methods for generating policy-relevant analysis and solutions. As a think tank, we identify and communicate realistic options to enhance effectiveness through evidence-based research on the causes, consequences and trajectories of insecurity and violence. We are operational because we design and conduct activities in complex and insecure environments.

About The Citizen Lab

http://www.citzenlab.org

The Citizen Lab is an interdisciplinary laboratory based at the Munk Centre for International Studies at the University of Toronto, Canada focusing on advanced research and development at the intersection of digital media and world politics. We are a *hothouse* that combines the disciplines of political science, sociology, computer science, engineering, and graphic design. Our mission is to undertake advanced research and engage in development that monitors, analyses, and impacts the exercise of political power in cyberspace. The Citizen Lab's ongoing research network includes the Information Warfare Monitor and the OpenNet Initiative, ONI Asia, and benefits from collaborative partnerships with academic institutions, NGOs, and other partners in all regions of the world.