Technical Report

UCAM-CL-TR-746
ISSN 1476-2986

Number 746

UNIVERSITY OF CAMBRIDGE

Computer Laboratory

The snooping dragon: social-malware surveillance of the Tibetan movement

Shishir Nagaraja, Ross Anderson

March 2009

15 JJ Thomson Avenue
Cambridge CB3 0FD
United Kingdom
phone +44 1223 763500

http://www.cl.cam.ac.uk/

Technical reports published by the University of Cambridge
Computer Laboratory are freely available via the Internet:

http://www.cl.cam.ac.uk/techreports/

ISSN 1476-2986

The snooping dragon: social-malware surveillance of the Tibetan movement

Shishir Nagaraja
Information Trust Institute
University of Illinois at Urbana-Champaign
sn275@iti.uiuc.edu

Ross Anderson
Cambridge University
Computer Laboratory
Ross.Anderson@cl.cam.ac.uk

Abstract

In this note we document a case of malware-based electronic surveillance of a political organisation by the agents of a nation state. While malware attacks are not new, two aspects of this case make it worth serious study. First, it was a targeted surveillance attack designed to collect actionable intelligence for use by the police and security services of a repressive state, with potentially fatal consequences for those exposed. Second, the modus operandi combined social phishing with high-grade malware. This combination of well-written malware with well-designed email lures, which we call *social malware*, is devastatingly effective. Few organisations outside the defence and intelligence sector could withstand such an attack, and although this particular case involved the agents of a major power, the attack could in fact have been mounted by a capable motivated individual. This report is therefore of importance not just to companies who may attract the attention of government agencies, but to all organisations. As social-malware attacks spread, they are bound to target people such as accounts-payable and payroll staff who use computers to make payments. Prevention will be hard. The traditional defence against social malware in government agencies involves expensive and intrusive measures that range from mandatory access controls to tiresome operational security procedures. These will not be sustainable in the economy as a whole. Evolving practical low-cost defences against social-malware attacks will be a real challenge.

1 Introduction

Following the Chinese invasion of Tibet, the Dalai Lama fled in 1959 to exile in India from where he has acted as the Tibetan spiritual leader and campaigned for Tibetan independence. His campaign has often embarrassed the Chinese government. In the run-up to the Peking Olympics of 2008, Tibet was particularly sensitive; bloody anti-Chinese riots in Lhasa and elsewhere in March 2008 were followed by a police crackdown involving many arrests and killings. The crackdown continues to this day.

The activities of the Dalai Lama and the Tibetan government in exile are coordinated by the Office of His Holiness the Dalai Lama (OHHDL) in Dharamsala. Most of its activities are quite overt and have to do with the Dalai Lama's diplomatic and campaigning work, including overseas trips, and his spiritual mission which ranges from religious festivals through pastoral care for Tibetan refugees to routine scholarly work.

Some of this work has of necessity a covert element. For example, a campaigning group such as the OHHDL may plan a publicity coup in secret for maximum effect. A tactical matter like this may require secrecy only for a few weeks or months, and the consequences of a leak are typically mild – loss of operational effectiveness.

However there are other covert matters where secrecy must be maintained for much longer, and the consequences of a leak may be severe. An example comes from schooling. While organising Tibetan-language schools in India or the USA is an open matter, such schools in Tibet itself may have to be covert. Their operation may place teachers' and even students' lives at risk. Indeed, everyone associated with the Tibetan movement who sets foot in Tibet or China is at risk of their lives. Another potentially sensitive information asset is a database of Tibetan refugees, including where they lived in Tibet, when they left and where they live now.

The OHHDL first started using the Internet to publish talks and speeches in the 1990s [1]. Since then, the use of IT in its daily activities has grown steadily. Email is now the staple means of communication within both the OHHDL and other arms of the Tibetan movement. Tibetans also generate a growing number of electronic documents in the process of scholarship and administration. Most of this is routine, but some documents are sensitive in the strong sense that they could be used to construct actionable intelligence for Chinese government agencies leading to fatal consequences for people in Tibet and China. In what follows, we will follow NATO practice and call such documents 'secret', while documents whose compromise will merely cause a loss of operational effectiveness (such as those relating to forthcoming political meetings) we will call 'confidential'. (In the past, the Tibetans did not differentiate between levels of sensitivity. Secret documents were sometimes sent by email; confidential documents still are.)

As in other organisations, the ease of communication brought by the Internet has shifted the social rules for information management. Many of the safeguards available in the world of paper files are much more difficult to implement in the electronic world in ways that provide both adequate strength of mechanism and acceptable usability. This raises the difficult and (now) urgent problem of what combination of technical controls and procedural measures are needed in the new world of online working.

2 Attacks on the Dalai Lama's Private Office

The OHHDL started to suspect it was under surveillance while setting up meetings between His Holiness and foreign dignitaries. They sent an email invitation on behalf of His Holiness to a foreign diplomat, but before they could follow it up with a courtesy telephone call, the diplomat's office was contacted by the Chinese government and warned not to go ahead with the meeting. The Tibetans wondered whether a computer compromise might be the explanation; they called ONI Asia who called us. (Until May 2008, the first author was employed on a studentship funded by the OpenNet Initiative and the second author was a principal investigator for ONI.)

Email users at the OHHDL have been suffering spam attacks for some time. While some of these are a part of a wider pattern of attacks on anyone plausibly associated with the Tibetan movement, others are specifically targeted at OHHDL users.

The web-hosting and email services used by the OHHDL are provided by a California company. A look at the email server logs revealed a number of successful logins from a range of IP addresses that belonged to Chinese and Hongkong ISPs, with which none of the OHHDL email users were associated. Given that there are fewer than 50 email accounts, the possibility of error or accident seemed low – and especially so as many of the suspicious source IP addresses belonged (according to APNIC) to ISPs operating not just in the Chinese mainland, but in China's Xinjiang Uyghur Autonomous Region, where police and intelligence units dealing with Tibetan independence campaigners are based.

Following discussions with the OHHDL, the first author travelled to Dharamsala in September 2008 to assist in a forensic investigation. A technical report on the background to this investigation, and on follow-up visits to Tibetan offices round the world by ONI Asia personnel, is published separately by ONI Asia and CitizenLab [2]. The purpose of this paper is to set out the technical findings of our investigation and discuss their wider implications.

We monitored the network traffic from the OHHDL to its mail service in California and immediately observed that gaining access to emails would have been straightforward for anyone who could monitor this circuit, since the traffic was unencrypted. The email server could be contacted via POP, IMAP and HTTP in insecure modes, with passwords and mail passing in plain text. We also noted that some passwords chosen by monks were easily broken with a dictionary attack using John the Ripper in about 15 minutes [3].

The 'standard' security-consultant advice might therefore have been that the monks turn on TLS encryption to their mail server, and adopt a password policy. However such a superficial diagnosis and prescription would not have given the Tibetans much of a defence. It turned out that the attackers used a different route.

2.1 The attack vector

Email attachments appear to have been the favoured strategy to deliver malicious payloads. This worked because the attackers took the trouble to write emails that appeared to come from fellow Tibetans and indeed from co-workers. The use of carefully-written email lures based on social context to get people to visit bogus websites has been called 'social phishing' [4]; in this incident, such email was used to spread malware and we therefore call this strategy *social malware*.

Subject: Kalon Tripa Succession
From: "Pema Rinzin" <prinzintibet@yahoo.com>
Date: Thu, September 18, 2008 8:14 am
To: choejor@dalailama.com

Dear Sir,

Attached please find the final Tibetan translation of my English announcement for the Kalon Tripa succession initiative. Response to my press release on September 2nd has been very positive and I have been receiving lots of email and phone messages from Tibetans everywhere.

I am trying to get someone to translate the Kalon Tripa Hochoe into English, but if you already have it translated, please send it to me.

Any advice from you in this initiative of mine would be greatly appreciated.

Yours sincerely,

Pema Rinzin
President
TAC

Official Photographer/webmaster
Office of His Holiness the Dalai Lama
Thekchen Choeling
P/O Mcleod ganj 176219
Dharamsala (H.P.)
India

Figure 1: One of the tampered emails used to spread malware

The initial break may have been facilitated by the fact that the monks in the OHHDL were not just engaged in administrative tasks but were also active on various discussion sites. A passive observer could easily note their names, their interests and the names of people with whom they interacted. Emails were sent to monks, purporting to come from other monks, but that had in fact come from outside. We assume that one monk clicked on an infected attachment, giving the attackers their first foothold. It is possible that the initial break came from somewhere else, such as a guessed password for the mail server, or a mail server compromise; but we did not see evidence of the pattern of compromise likely after a passive wiretap, or of malware attacks on the mail servers themselves. We assess that the attackers probably used publicly-accessible mailing-list archives to construct the social-malware emails that they sent to their first targets.

Our analysis strongly suggested that once they has secured an initial foothold, the attackers gained access to the mailboxes of several users at the mail server. The successful logon attempts from China recorded from the mail server log point to this. They then used social engineering based on the contents of internal emails to expand this compromise to infect many other machines at the OHHDL. In particular, they targeted the email addresses of prominent members of the OHHDL and of key support staff including the system administration team.

An interesting and very effective twist was that the attackers did not just use the social information they gained from their initial attack to send plausible phish. They also stole mail in transit and replaced the attachments with toxic ones. Figure 1 shows an email whose body was stolen from the mailbox of a user and then used to construct the attack by attaching a malicious payload.

2.2 The payload

Our next observation concerns the malware payloads used. These were packaged as either .doc or .pdf files that installed rootkits on the machines of monks who clicked on them. During our initial network monitoring exercise, we observed sensitive files being transferred out of the OHHDL using a modified HTTP protocol: the malware picked up files from local disks and sent them to three servers which, according to APNIC, were in China's Sichuan province, using a custom protocol based on HTTP. The malware uses HTTP GET and HTTP POST messages to transfer files out and also appears to verify successful transmission. Sichuan, by the way, is the location of the Chinese intelligence unit specifically tasked with monitoring the OHHDL.

We then examined samples of email attachments from the local filesystems with the expert help of Mikko Hypponen at F-Secure Corporation, who determined that they could support file search and retrieval operations and also function as keyloggers. This confirms that the attackers had pretty much full access to the data on the infected computers. (In fact, one monk claimed that he actually 'saw' the bot open his Outlook Express and send infected attachments to others without any action on his part!)

2.3 The attackers' operational security

We initially expected that the attackers would seek some form of anonymity, perhaps by attacking through intermediate relays, or maybe an anonymity service such as Tor [5] – the largest such system. But a comparison of the IP addresses used in the attack with Tor exit node IP addresses (both in China and elsewhere) proved negative.

However, after a while, we saw a number of accesses through Dynaweb – a set of anonymisation proxy servers associated with the Falun Gong religious movement, which is also detested by the Government of China. We are at a loss how to explain this. Perhaps the Chinese detected the start of our clean-up operation and decided to hint that they had compromised Dynaweb – whether to deter people from using it, or to deter the US government from funding it? We just have no idea.

With hindsight, the Tibetans were fortunate in that the Chinese made the operational error of using surveillance product for a minor and tactical diplomatic purpose. By demonstrating that they had access to confidential data, they alerted the OHHDL to worry about the secret data too. This underlines the wisdom of the traditional NATO doctrine of treating communications intelligence product as Top Secret Codeword and enforcing very severe restrictions on its use.

3 Analysis and Countermeasures

The informal security model used at the OHHDL (as in most companies) was essentially one of discretionary access control: users were trusted to use computer resources sensibly. Yet we observed users storing secret documents on the local filesystem of a computer also used for risky activities such as browsing the Internet and opening emails with attachments from colleagues (actually strangers pretending to be colleagues). The handling of sensitive data was thus inadequately separated from risky activities – activities that require the user to trust content from strangers.

Next, although the attacks we document here came from the intelligence services of a major country, there is nothing in the modus operandi that prevents them from being carried out by a smaller opponent. For example, we saw no evidence that the initial break involved wiretapping the backbone traffic from Dharamsala to California – the kind of exploit popularly associated with a large-country agency. There was no need, given the tools and methods they actually employed. In fact, even a capable motivated individual could have carried out the attacks we describe here. Until recently, one might have assumed that it would take a 'geek' to write good malware, and someone with interpersonal skills to do the social manipulation. But the industrialisation of online crime over the past five years means that capably-written malware, which will not be detected by anti-virus programs, is now available on the market. All an attacker needs is the social skill and patience to work the malware from one person to another until enough machines have been compromised to complete the mission. What's more, the 'best practice' advice that one sees in the corporate sector comes nowhere even close to preventing such an attack.

Thus social malware is unlikely to remain a tool of governments. Certainly organisations of interest to governments should take proper precautions now, but other firms had better start to think about what it will mean for them when social malware attacks become widespread. What Chinese spooks did in 2008, Russian crooks will do in 2010, and even low-budget criminals from less developed countries will follow in due course.

So what are the broader implications? How can social malware be dealt with?

3.1 Countermeasures for NGOs

The first question is what defences are available to an organisation such as the OHHDL. The world of defence computing gives us a workable, if very expensive, answer. It starts with the use of mandatory access controls (MAC) to provide strong separation of processes and data. At its simplest, the Bell-LaPadula model ensures that information may flow up from Low to High but not down; this is also known as multi-level security (MLS). An immense research programme, lasting over thirty years, led to the creation of software products and an assurance infrastructure to support this model; a good introduction may be found in [7]. Until recently, high-grade MAC/MLS products were not available to normal users and were even export-controlled; but now products such as Trusted Solaris and SELinux are available without restriction. But could a typical organisation use these tools effectively?

The classical MAC/MLS approach to the Tibetans' protection problem would start with a system of information classification, as we discussed already. A firewall or mail guard implemented on an SELinux platform might be used to ensure that no secret documents are made available to resources at a lower level, such as a machine on which external email or web pages had been read. And clearances matter as well as classifications. Access to secret documents would be restricted to staff who have at the very least had a background check – otherwise Chinese agents can simply walk over the border from Tibet and volunteer to work at the OHHDL.

Then there's the hardest part – operational security. How do you train your staff so that they won't fall prey to social engineering attacks? An old NSA security manual that fell into the public domain in the early 1990s gives some insight of the lengths that the

agencies go to to prevent hostile agencies targeting their staff [8]. The emphasis is not just on discretion but on anonymity. This again is sound advice for any organisation that handles real secrets – only a handful of carefully-chosen people should have access to the secrets, their names should not be public, and they should have a low profile online. However, it is against the Dalai Lama's policy to have any secret organisations.

Finally there's the red team. It's important to test your defences; we discovered the extent of the compromise rapidly when we started monitoring the traffic to and from the OHHDL. One technique is to probe your operational security. Phone up your own organisation and see what you can extract with just a little bit of guile; Mitnick's book has lots of ideas to work with [9]. But there are limits on the level of operational security that can be sustained outside the world of defence and intelligence. Most companies would rather not teach staff to be (even more) unhelpful to customers and to each other, and few religions would want to train their headquarters staff to be rude to the faithful. Where there is a dedicated cell of people handling secret data, the regular operational security testing effort should be directed at them. The organisation as a whole should place greater emphasis on monitoring outgoing traffic to see whether anything is escaping that shouldn't, such as the names (or cover names) of staff involved in field work, and of some of the people in the refugee database.

Overall, our fieldwork brought home to us that a small organisation with few secrets, such as the OHHDL, is likely to find the engineering costs and administrative overhead of doing multilevel security to NSA standards to be unsustainable. It is much more practical to keep the secret data on machines in a separate building with no network connection – or better still, to work with pen and paper. The access control, opsec and network monitoring can become much more manageable if secret data are kept away from network-attached computers.

3.2 Countermeasures for companies

What happens when criminals start using social malware to attack companies? No-one should think that it could not happen to them, just because their company is in New York or London rather than an Indian hill station! The Tibetan sysadmins were just as capable as one finds in the USA or Britain. Indeed, they were probably more aware of the Chinese threat and as a result more alert than a typical company security team. They observed that a security compromise might have taken place, and called expert help. Furthermore, they have permitted us to document what happened. All in all, the Tibetans' performance has been more effective than we would have expected from a randomly-chosen Western organisation.

There have been reports before of Chinese industrial espionage against defence companies in the West, notably the 2008 annual report of the U.S.-China Economic and Security Review Commission, according to which U.S. government agencies and defence companies have had their unclassified networks compromised by Chinese hackers [11]. But the evidence they heard on these attacks was classified, and their report lacks the technical detail that we provide here. A fuller (if still non-technical) story is told by U.S. military expert Timothy Thomas, whose book tracks the history of Chinese information warfare doctrine [10]. According to Thomas, Chinese strategic thinkers consider that a state of information warfare already exists between them and the West; in an extension of the

Cold War, the West is already attacking China by exporting subversive ideas to it over the Internet. Both the attack on the Tibetans described here, and the industrial espionage attacks described elsewhere, are consistent with the picture Thomas paints.

In view of continuing concerns about industrial espionage, strict separation is indeed practiced in some sectors. We are aware of one company that maintains totally separate networks for design work and external communications; the typical lab has PCs that connect to the CAD/CAM system, and PCs of a different colour that connect to the Internet. Draconian physical and procedural controls try to prevent data leakage from one network to the other. But while such arrangements may be sustainable in a cost-plus defence-contracting environment, they are too expensive for the normal economy.

So what will happen when normal criminals start using social malware to steal money from normal companies?

A typical medium-sized company, or an operating division of a large company, might pay several thousand employees and tens of thousands of invoices every month. So payments must be automated. Typically this involves an accounting package feeding a payment application supplied by the company's bank. A crook could target the payment PC directly, or proceed indirectly by taking over the PC of an accounts payable clerk or payroll clerk in order to input false data to the accounting system.

It is possible to make payment systems malware-proof. Twenty years ago, the second author worked at a bank that used a cash-management system consisting of an application that was run on a PC XT from a write-protected floppy disk that also contained a copy of the operating system, supplied by the bank. This was a good design; it turned the PC into a payment appliance and excluded the simultaneous use of any other software, including malware. Unfortunately, it has been downhill all the way since then! It would in our view be prudent practice to run a high-value payment system on a PC that does not contain a browser or email client, or indeed any other software at all. Perhaps within a few years banks will insist on this, and design payment applications that won't run otherwise. (Microsoft sells a stripped-down version of Windows for use in ATMs; perhaps their market is about to grow.) Perhaps a few years later we will see the payment function becoming a hardware appliance: a tamper-resistant device supplied by the bank that does nothing except display payments and signs them when the approval button is pressed. Cryptographers have mused about such systems for years; perhaps social malware will at last provide their killer application.

Designers of accounting systems will also need to make more pessimistic assumptions. At present such systems are designed to deal with the presence of a single dishonest insider, using mechanisms for separation of duty and audit. Their vendors may take the view that a single infected PC is no worse than a dishonest member of staff. But it is in the nature of social malware that a successful attack is likely to compromise many of the machines in an office. The implications will require careful study. Banks have a hard enough time coping with the effects of phishing, where the computers of less than 1% of customers may be under hostile control at any one time [12]; how can you run an accounting system if half the machines are under hostile control? Will it be possible, for example, to anchor internal controls on a hardened payment PC? Or should companies insist that accounting staff use separate PCs for accounting and for email? Initial discussions with accounting staff suggest that this would be very tiresome. Is virtualisation the answer? Within a few years, we may have to find out.

One thing we predict, though, is that the social response to the threat of social malware will be slow and ineffective. This is because of elementary security economics [13]. Banks will try to shift the blame to accounting system providers, and vice versa. The accounting vendors will advise customers to lock down user PCs, without being too explicit about how. Companies seeking redress will find themselves up against standard terms and conditions whereby both banks and vendors disclaim liability; in many markets they are oligopolistic suppliers, so may be able to defend these contract terms for some time. The banking regulators have shown that they believe whatever the banks tell them, that they are uninterested in protecting bank customers, and in any case they have no expertise in information security. The initial attacks will affect only a minority of firms, so the rest will prefer to blame the attacks on the victims' negligence rather than acknowledging that their own policies need to change. Many companies will rely for advice on their auditors, and big audit firms, being ponderous and bureaucratic, give the same advice year-in year-out until litigation or regulation forces change. In short, we predict that the criminals who adapt social malware to fraud will enjoy many years of rich pickings. Indeed, if either of us were inclined to crime, this would be what we'd go for.

4 Conclusions

In this note we described how agents of the Chinese government compromised the computing infrastructure of the Office of His Holiness the Dalai Lama. They used social phishing to install rootkits on a number of machines and then downloaded sensitive data. People in Tibet may have died as a result. The compromise was detected and dealt with, but its implications are sobering. It shows how difficult it is to defend sensitive information against an opponent who uses social engineering techniques to install malware.

We have described this *social malware attack* here and considered its consequences. Although the attack we describe in this case study came from a major government, the techniques their agents used are available even to private individuals and are quite shockingly effective. In fact, neither of the two authors is confident that we could keep secrets on a network-connected machine that we used for our daily work in the face of determined interest from a capable motivated opponent. The necessary restrictions on online activity would not be consistent with effective academic work.

Organisations that maintain sensitive information on network-attached computers and that may have such opponents had better think long and hard. The implications are serious already for people and groups who may become the target of hostile state surveillance. In the medium term we predict that social malware will be used for fraud, and the typical company has really no defence against it. We expect that many crooks will get rich before effective countermeasures are widely deployed.

Acknowledgements: The first author is supported by a generous grant from the I3P Consortium. We are also grateful to a number of colleagues, some of whom wish to remain anonymous, and most of all to the Office of His Holiness the Dalai Lama for permission to write this report so that others may learn from their experience. Established governments appear unwilling to discuss their experience of such attacks; the Tibetan openness is by comparison truly enlightened.

References

[1] http://www.tibet.com was already active when http://www.archive.org opened spidered it in 1996; http://www.tibet.net has been active since 2001

[2] "Tracking Ghostnet: Investigating a Cyber Espionage Network", in *Information Warfare Monitor* JR02-2009, 29 Mar 2009

[3] http://www.openwall.com/john/

[4] "Social phishing", Tom Jagatic, Nathaniel Johnson, Markus Jakobsson, Filippo Menczer, in *Communications of the ACM* v 50 no 10 (Oct 2007) pp 94–100

[5] "Tor: anonymity online", at http://www.torproject.org/

[6] "Dynaweb", at http://www.dit-inc.us/dynaweb

[7] *'Security Engineering – A Guide to Building Dependable Distributed Systems'*, Ross Anderson, Wiley 2008

[8] *'The NSA Security Manual'*, at http://www.cl.cam.ac.uk/~rja14/Papers/nsaman.pdf

[9] *'The Art of Deception: Controlling the Human Element of Security'*, Kevin Mitnick, William Simon and Steve Wozniak, Wiley 2002

[10] *'Dragon Bytes: Chinese Information-War Theory and Practice'*, Timothy L. Thomas, Foreign Military STudies Office, Fort Leavenworth, Kansas, 2004

[11] *'2008 REPORT TO CONGRESS of the U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION'*, 110th Congress, Nov 2008, at http://www.uscc.gov/annual_report/2008/annual_report_full_08.pdf

[12] "Closing the Phishing Hole – Fraud, Risk and Nonbanks", Ross Anderson, at *Nonbanks in the Payment System*, Santa Fe, NM, May 2007; available from http://www.ross-anderson.com

[13] *'Security Economics and the Internal Market'*, Ross Anderson, Rainer Böhme, Richard Clayton and Tyler Moore, ENISA, March 2008; shortened version in *Workshop on the Economics of Information Security* (WEIS 08); available from http://www.ross-anderson.com