DIGITAL DISRUPTION:

EXPLORING THE IMPACT OF CYBER ATTACKS ON THE TIBETAN COMMUNITY IN EXILE

TIBCERT

Published By:
Tibetan Computer Emergency Readiness Team (TibCERT)
10 December, 2024

Tibet Action Institut
བོད་ཀྱི་ལས་འགུལ་བཟོ་གནས་ཁང་།

CONTENTS

INTRODUCTION

A young Tibetan woman living in Northern India takes a trip back to her village in Tibet to visit family. For the last two years she has been working for Drelwa, a Tibetan NGO that provides ways for Tibetans inside Tibet to connect with the diaspora online. The trip does not go as planned.

When she reaches the Nepalese-Tibetan border she is immediately taken into detention and held for two months. Chinese authorities interrogate her about her employment in Dharamsala. The young woman denies being involved in any political activities and insists she went to Dharamsala for studies. The authorities presented a stack of chat transcripts from conversations she has had online. They explained to her that they have been monitoring Drewla and knew about its activities. They eventually released the woman and allowed her to travel to her village with a message for her colleagues back in Dharamsala: "You are not welcome to return to Tibet".

Drewla was indeed under surveillance. Researchers at the Citizen Lab at the University of Toronto ran an investigation into the networks of Drewla and other Tibetan organizations in 2009 and found that they were all infected by malware that connected to GhostNet, a digital espionage network.[1] The goal of GhostNet was to maintain clandestine access to computer networks and communications for as long as possible.

Tibetans were not the only targets. GhostNet infiltrated over a thousand computers in over one hundred countries around the world. The command and control servers used to operate the malware were traced back to China, and the targets all had a common connection: geopolitical interest to the People's Republic of China (PRC). Exposing this network revealed to the world a dark truth that Tibetans had known for years: China uses targeted malware as a form of digital espionage to spy on its opponents.

The Tibetan community has been targeted by digital espionage for over 20 years by groups with ties to the PRC. These coordinated campaigns aim to infiltrate the communications and data of key people and organizations in the Tibetan community to disrupt and subvert the goals of the Tibet movement.

This type of spying violates rights to privacy, assembly, and free speech. Digital espionage is a form of transnational repression that extends the reach of authoritarian states beyond their borders to surveil, harass, and intimidate political dissidents and marginalized groups. By infiltrating digital communications and preemptively identifying dissent, the PRC aims to counteract any challenges to its authority, both domestically and internationally.

Digital espionage campaigns against the Tibetan movement have been widely documented by threat intelligence

1 https://citizenlab.ca/wp-content/uploads/2017/05/ghostnet.pdf

companies and research groups.[2] Missing from these reports are the voices of the community and discussion of how decades of digital spying impact the movement.

The arduous history of digital espionage against the Tibetan community acts as a canary in the coal mine for global civil society. The experience of the Tibet movement provides a warning that harnessing the power of information technology for social movements requires vigilant attention to digital security.

This report documents the history of digital espionage against the Tibetan community through first hand accounts of targeted people and groups. These stories reveal the harms of digital transnational repression and show how the Tibetan movement has built capacity to defend against the threat. The Tibetan community has taken ownership of the challenges it faces online developing digital security training, capacity building, and incident response capabilities. These efforts culminated in 2018, when the Tibet Action Institute launched the Tibetan Computer Emergency Readiness Team (TibCERT), which seeks to foster collaboration on digital security in the Tibetan community, respond to security incidents, and provide Tibetans in Tibet with the latest information on censorship and surveillance. TibCERT is a natural progression of the digital security work that Tibet Action Institute had been carrying out in the community for over a decade.

The stories shared in this report present the harms of digital threats while also offering a message of empowerment, which shows how social movements can persevere in the face of authoritarianism and continue to speak truth to power.

The report is structured in three sections outlined below:

BACKGROUND

This section recounts the early history of how the Tibetan movement came online and the digital threats that soon followed.

VOICES FROM THE COMMUNITY

This section shares stories from members of the Tibetan community who have been targeted by digital espionage. Their testimonies document the history and impact of digital threats against the Tibet movement.

THE COMMUNITY RESPONDS

This section describes the remarkable digital resilience built by the Tibetan community in response to digital espionage and reflects on what civil society can learn from this experience.

2 Cyber Espionage Against Tibetans: An Analysis of over Two Decades of Publicly Available Data

BACKGROUND

This section tells the early history of how the Tibetan movement came online and the digital threats that soon followed.

THE TIBET MOVEMENT GOES ONLINE

Dharamshala, a small city in Northern India has been the central hub of the Tibetan diaspora since His Holiness the Dalai Lama made it his residence after escaping from Tibet in 1959.

Before 1995, the Tibetan community relied on Internet connectivity set up in India by the United Nations called "ERNET" (Education and Research Network). Accessing email required going to the roof of the Nathang Parkhang building where the Tibetan Computer Resource Centre (TCRC) office was located, where there was a single computer available. TCRC is a department of the Tibetan Government-in-Exile (TGiE, now known as the Central Tibetan Administration, CTA) that provides technical resources and technical support to all other departments. At the time, there was only one email address for sending or receiving email for the entire community.

Then, in the mid-1997, the community truly came online under the administration of TCRC and with the support of an American, Dan Haig, who did early work on the World Wide Web in California. Dan had initially traveled to Dharamsala to study Tibetan medicine, however given his technical expertise he soon found himself helping the Tibetan Government in Exile connect to the Internet.

"In January of 1996, I registered tibet.org, which marked the beginning of my involvement with the Tibet movement. Unexpectedly, this journey led me to various places I had never envisioned. Concurrently, I maintained communication with Phuntsok Namgyal [the Manager at TCRC].

About a year and a half later, I found myself in India with four companions, equipped with everything necessary to establish a network connecting all the offices in Gangkyi [The colloquial physical location name in Dharamsala where Tibetan Government in Exile is based].

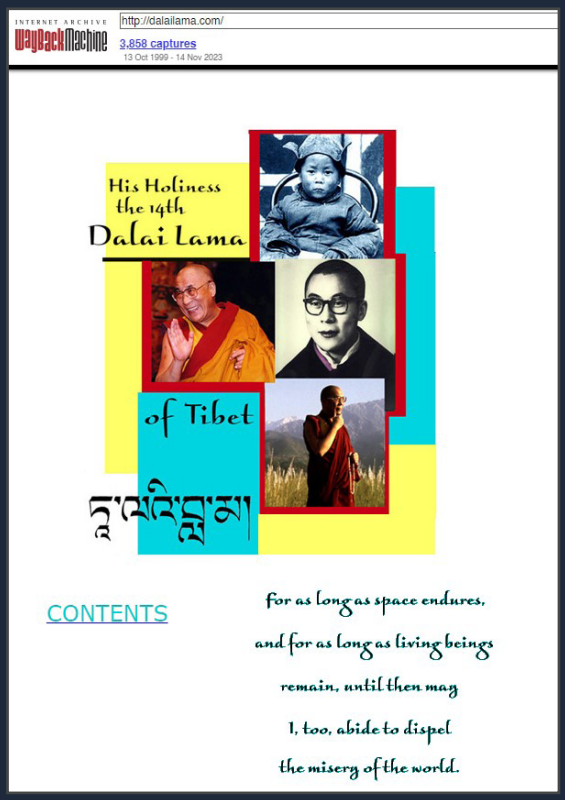
This network facilitated a dial-in connection from the Private Office of His Holiness the Dalai Lama and Norbulingka Institute, among other locations.

Our goal was to usher the Tibetan exile community and the government-in-exile into the Internet age."

- Dan Haig (COO, InteLex)

Dan and his friends, together with the TCRC, helped the TGiE set up an Internet-connected Local Area Network between the Kashag (highest executive office of TGiE), all seven ministries of the TGiE , the

Library of Tibetan Works and Archives, and provided connectivity to the Private Office of His Holiness the Dalai Lama (OHHDL), the Norbulingka Institute and other key community organizations.[1]



On December 18, 1996, the website DalaiLama.com was registered.[2] At that time, monks from the OHHDL were managing the Office's email, maintaining databases, hosting the website, and managing the content. The OHHDL used email to schedule His Holiness' meetings with international diplomats and religious leaders around the globe.

DalaiLama.com webpage from 1999 archived online[3]

In 2000, the official website of the TGiE (tibet.net) was established and the TGiE network consisted of over 120 computers. [4]

It was also around this time that the wider Tibetan community both in India and abroad started to come online. However, as the community came online, information security threats followed.

Dan Haig recounts how even at this early stage of Internet connectivity, digital espionage emerged.

"During that time, we faced minimal hacking issues ourselves, but the Chinese government initiated a deceptive tactic. They began sending emails, spoofing legitimate addresses and claiming they had been compromised. For instance, an email purportedly from me, Daniel D. Haig, was circulated to the Tibet Support Groups list. However, it was poorly written and signed as 'Haig D Daniel,' which was obviously fake since I typically sign my emails with just a dot and a 'D.'

Despite the obvious forgery, they refined their approach, enticing recipients to click on links leading to websites hosting malware. Subsequently, they launched an extensive campaign, distributing emails with malicious attachments. Clicking on these attachments would infect computers, leading to a myriad of potential consequences."

- *Dan Haig(COO, InteLex)*

Information technology has always been a double-edged sword for the Tibetan community. On one hand, it has significantly contributed to strengthening the Tibetan freedom movement, fostering greater communication opportunities between Tibetans in Tibet and the outside world, and promoting awareness of Tibetan Buddhism and culture on a global scale. However, alongside these advancements, the community has become increasingly vulnerable to online threats orchestrated by groups affiliated with the PRC. Exploiting the community's relatively limited

1 Dan Haig - How the internet came to Dharamsala

2 Source: https://who.is/whois/dalailama.com (accessed December 8, 2022).

3 Original website archived here: https://web.archive.org/web/19991013110002/http://dalailama.com/ (accessed December 8, 2022).

4 https://web.archive.org/web/20150626144441/http://www.tibetangeeks.com/geeks/history/how_the_internet_came_to_dhasa_tibetans-dan_haig-20130927.html

information security capacity, these groups infiltrate communication networks, surveil individuals and organizations, and continue to pose significant challenges to the integrity and security of the Tibetan movement.

EARLY DIGITAL THREATS AGAINST THE COMMUNITY

One of the earliest documented incidents of digital espionage against the community was reported in September 2003 by Jigme Tsering, a manager of the Tibetan Computer Resource Centre.[5]

"A number of targeted computer viruses circulating via email throughout the Tibetan Government in Exile and Tibetan support groups and related Non-Government Organizations have been discovered or brought to our attention.

These viruses have appeared in a number of variants, indicating a progressive and sustained development process. For example, some were taking advantage of known security loopholes in Microsoft software in order to automatically run and are always personalized to impersonate departmental emails following previous attempts to collect email address lists. One variant analyzed was found to have been sourced from the Yunnan Province in China, and was designed to collect information of an infected computer and send it via email to an address in Beijing."

- Jigme Tsering(Representative for Office of Tibet, South America)

Targeted malware delivered as file attachments to email messages is one of the most common digital espionage tactics experienced by the Tibetan community.

Targeted malware operations typically consist of the following process: The targeted user receives an email, possibly appearing to be from someone they know with a message—sometimes specific, sometimes generic—that urges the user to open an attachment, usually a PDF or Microsoft Office document or visit a website.

If the user opens the attachment or link with a vulnerable version of software that has been targeted for exploitation and no security mitigations are in place, their device will likely be compromised. 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. Once the user's computer is compromised, operators can extract documents, email and other data, and possibly move laterally through the compromised network to target other devices.

Research conducted into the decades of digital espionage against Tibetans has shown that – as a community – Tibetan civil society faces the same level of information security threats as major companies and governments, but with far fewer resources to defend against them. This stark reality was first revealed in 2009, when the Information Warfare Monitor (a collaboration between the Citizen Lab and the Secdev Group) published the report "Tracking GhostNet."[6] The investigation started as a probe into key Tibetan organizations to determine if they were compromised by digital espionage. The result was uncovering the GhostNet digital espionage network that compromised the Offices of HHDL and other Tibetan groups, alongside 1,295 computers in 103 countries around the world – 30% of which can be labeled

5 "Chinese Internet group found spying on Tibetan government computers", International Campaign for Tibet, October 28, 2003.

6 "Tracking Ghostnet: Investigating a Cyber Espionage Network", Citizen Lab, March 29, 2009

as "high value" targets such as Ministries of Foreign Affairs and Embassies. The investigation traced the command and control servers used to issue commands to compromised machines back to locations in China. However, the researchers were unable to conclusively determine the potential role of the government. What was evident is that this network was performing politically motivated espionage targeting both civil society and governments. From the perspective of the Tibetan community the culprit was clear, it was the government of China.

When the GhostNet report was released, there were almost no public reports on digital espionage. In subsequent years public reporting from the Threat Intelligence industry grew considerably and served as marketing material for companies. In general these reports focus on threats to governments and the private sector which represent the customer base of the industry. Civil society is seldom the focus of these reports with an important exception, the Tibetan community.

In the accompanying report "Cyber Espionage Against Tibetans: An Analysis of over Two Decades of Publicly Available Data[7], TibCERT systematically reviewed threat intelligence reports from 2009 to 2022 and found 63 reports[8] which documented digital espionage against the Tibetan community. These reports are primarily focused on technical analysis of the malware threats and do not address how they affect the targeted individuals and organizations. Although there is a significant amount of publicly available reports of targeted espionage campaigns against the Tibetan community, we believe that this volume of public reports may not be the only reports available as it is likely plausible that threat intelligence companies may have a lot more internal reports that are not shared publicly.

The malware used in these campaigns often mirrors digital espionage activities originating from China that target governments and the private sector. Therefore, reporting on cyber threats against Tibetans do provide threat intelligence companies a way to publicly disclose details about the modus operandi behind these cyber attack campaigns without having to disclose any sensitive incidents or customer data. This phenomenon has amplified the coverage of cyber threats against the Tibetan diaspora community from threat intelligence companies among other civil society movements and oppressed minorities. These reports provide useful technical information and serve as evidence of decades of targeted espionage. However, typically these private sector reports are done without involvement of the Tibetan community and rarely provide any notifications or incident response support to targeted individuals and groups.[9] Therefore, while the reports provide value to companies, the Tibetan community does not receive any direct support.

---

7 Cyber Espionage Against Tibetans: An Analysis of over Two Decades of Publicly Available Data

8 The reports were selected based on their clear references to cyber attacks against Tibetan diaspora community ever since the 2000s, published by academic institutions and cyber security companies namely Citizen Lab (University of Toronto), Kaspersky, Trend Micro, Palo Alto Networks , AT&T Alien Labs, Proofpoint, Recorded Future, and Security Week. We ensured the reports included more technical details to ascertain the level of effort put behind these attacks, tactics deployed in the attacks, evolution of these threats over time and what inferences we can make to understand who these threat actors are and what their motivations could be.

9. An important exception is the work of the Citizen Lab at the University of Toronto, which was a key partner in the GhostNet investigation and subsequently spent over a decade documenting threats to the Tibetan Community. This academic research included direct involvement of the community and sought to increase digital security knowledge and capacities of targeted groups. There are also instances of private sector companies attempting outreach to the Tibetan community to report compromise. Prior to the launch of TibCERT this outreach was very difficult as companies did not know how to reach targeted groups and there was no central hub to share information. TibCERT helps facilitate communication and coordination between private sector companies with threat information and targeted groups.

VOICES FROM THE COMMUNITY

While incidents of digital espionage against the Tibetan community are well documented in threat intelligence reports, the focus is almost always on the technical aspects alone. These reports provide little analysis or understanding of the social and political context in which these threats occur. Without this context, it is not possible to understand the harm of digital espionage to those it targets.

Only paying attention to the malware and other technical tricks being used in digital espionage is like investigating a shooting but only analyzing the gun but ignoring the victim or the crime scene. When gun crime is investigated, the forensic details of the bullet may help connect similar attacks and maybe even trace it to the shooter, but if the damage against the victim and the context in which the attack happened is ignored the nature and impact of the crime cannot be properly assessed. Digital espionage is no different. A full understanding of digital espionage requires a wider and deeper view into the issue.

We interviewed members of the Tibet movement who have been targeted by digital espionage to document the history and impact of digital threats against the Tibet movement, as well as the remarkable digital resilience built by the community in response.

We organized the stories we collected from the community into two sections.

The first section shares stories from Tibet leaders and groups that have come under digital surveillance during key moments for the Tibetan movement including the 2008 Beijing Olympics, the wave of self-immolations in the mid 2000s, and the COVID-19 pandemic.

The second section describes different forms of digital threats that Tibet supporters have experienced from malicious email campaigns that impersonate Tibetan groups, espionage campaigns that compromised Tibetan websites and use them to serve spyware to visitors, attacks aimed at censorship rather than surveillance, and finally digital espionage targeting phones.

Together these sections show the history and evolution of digital espionage against the Tibetan community from the perspective of the community.

SPYING DURING PIVOTAL MOMENTS FOR THE TIBET MOVEMENT

The first line of attack in most digital espionage that uses targeted malware is luring targets to perform some kind of action, usually opening a malicious attachment or link. The social engineering tactics used in these intrusion attempts are often highly sophisticated and show a knowledge of the activities and network of the target. This level of sophistication speaks to the effort being put into the espionage campaigns and the amount of information the adversaries already have on their targets.

The stories we collected are from individuals involved in Tibet advocacy key moments in the history of the Tibetan freedom movement. The mirroring of these major events with spikes in online attacks targeting the community reflects how closely the PRC monitors the community and the persistence of digital threats over two decades.

SURVEILLANCE, HARASSMENT, AND THE 2008 BEIJING OLYMPICS

In 2008, Beijing played host to the Summer Olympics. The mega event was a major publicity moment for the government of China and accordingly was also a crucial moment to bring attention to its perpetration of human rights abuses against Tibetans and other targeted communities.

A wave of unprecedented protests broke out across Tibet against China's occupation and unceasing violations of Tibetans' basic rights and freedoms. During this uprising, many Tibetans and non-Tibetan allies working with Tibet Support Groups conducted advocacy work and solidarity protest actions including disrupting the Olympic Torch routes as well as highlighting the dire situation inside Tibet on international media platforms and to global decision makers.

Kate Woznow was part of this advocacy effort as Campaign Director of Students for a Free Tibet. From Bangkok, Thailand, Kate coordinated a flurry of activities including organizing protests and managing media strategies. During this period Skype was a key communications tool for Kate to reach activists across the world from Beijing, London, New York and beyond. These communications were often highly sensitive and Kate and her colleagues took precautions such as using code names to mask their identity. Despite these efforts Kate soon found herself a target of surveillance and harassment.

In August 2008, as the Olympics games opened Kate began to receive suspicious Skype messages. The person on the other end addressed her by the code name she has not used publicly and also knew the code name for Kate's colleague Lhadon Tethong, Executive Director of Students for a Free Tibet. The messages were written in a tone to suggest that the person already knew Kate. They asked if she was in Hong Kong and asked scoping questions about what she was doing there and if she was interested in business opportunities. This attempt to uncover her location was particularly alarming, as Kate had briefly been based in Hong Kong in 2007 while coordinating media coverage of a protest in Beijing. The protest had targeted the Chinese government's decision to summit the Tibetan side of Mount Everest with the Olympic torch.

"It was unnerving to have people on my Skype who knew my code name and who seemed determined to seek out my location. They were clearly doing this to intimidate me and others involved in the protests and to let us know that they knew were …

There was a thuggishness to the tone of the messages that reminded me of other in-person situations I'd faced with Chinese authorities. It was evident they were transferring their tactics of intimidation online and trying to shut us down by revealing that they could infiltrate our online spaces and potentially disrupt our advocacy work. I recall thinking how unbearable it must be for Tibetans in Tibet to have to live under under this regime of online surveillance and harassment."

- Kate Woznov (Director, Tibet Action Institute)

SPYING AND SELF IMMOLATIONS IN TIBET

In the aftermath of the 2008 Beijing Olympics, Chinese authorities waged a brutal crackdown in Tibet, leading to arrests of thousands of Tibetans and the deaths of over 100 Tibetans[10]. Beyond those involved in the 2008 protests, Tibetan writers, singers, and educators became prime targets of repression.[11] A report from the International Campaign for Tibet (ICT) published on March 9, 2009 revealed that around 600 Tibetans have been detained as political prisoners since March 2008. [12]

2009 marked a somber turn for Tibetans when a 20-year-old monk from Kirti monastery named Lobsang Tashi (or Tapey to his friends) self-immolated in protest against Chinese policies. As his body burned in protest, Chinese police shot him and took him into custody.[13] His protest was understood as a plea for international attention to China's oppressive measures in Tibet.

Over the next nine years, 158 more Tibetans self-immolated, calling for the return of His Holiness the Dalai Lama and freedom for Tibet. This unprecedented series of self immolations was a major turning point for the Tibet movement as it demonstrated the extreme levels of repression Tibetans in Tibet were under and the measures they were prepared to take to bring attention to the dire human rights situation.

During this time, like all leaders in the Tibet Movement, Lhadon Tethong, the Director of Tibet Action Institute paid close attention to the self-immolations and worked tirelessly to bring international attention to them.

In February 2012, Lhadon received an email that appeared to come from Cheng Li, a notable Chinese-American scholar who was Director of Research at The Brookings Institution, a Washington DC-based think tank. In the email, Mr. Li explained to Lhadon that he would be attending an academic conference on religious research in Shanghai and would like to learn more about Tibetan self immolations. The email included a spreadsheet that Mr. Li explained listed Tibetans who had self-immolated since 2009. He asked Lhadon to review the document for him.

10. "Tibet Protest 2008", International Tibet Network
11. A Raging Storm", International Campaign for Tibet, May 19, 2010
12. A Great Mountain Burned by Fire: China's Crackdown on TIbet", International Campaign for Tibet
13. Remembering the First Person Who Self-Immolated Inside Tibet, Tapey" by Woeser", High Peaks Pure Earth, March 8, 2012

On the first read Lhadon was enthusiastic about this request from a prominent China expert. However, she quickly determined that the email was not sent from the real Cheng Li. A telltale sign was that the email was sent from a suspicious looking email account (chengli.brookings@ aol.com).
As a leader in the Tibet movement Lhadon had become accustomed to receiving emails with malicious files and messages designed to entice her to open them. The constant targeting she experienced made her weary of any messages she received. While these types of emails were routine to Lhadon, this particular message left her feeling vulnerable.

"I remembered thinking that this was good, a well crafted, researched targeted attack and I wouldn't say I was impressed but maybe my blood ran a little cold recognizing how sophisticated cyber attacks can be and there was no question to deny that it must be a Chinese government backed attack."

- Lhadon Tethong
(Director and Co-founder, Tibet Action Institute)

Lhadon sent the email to researchers at the Citizen Lab who verified the attachment contained malware designed to infect computers running Windows.[14] This finding confirmed Lhadon's suspicions the email was a clever attempt at breaking into her computer and spying on her.
Following this revelation, Lhadon and the Citizen Lab researchers devised their own ruse to turn the table on the attackers. Lhadon wrote back to "Cheng Li" with some information about the type of computer she was using as bait that the attackers may be interested in.

> *"Thank you for your inquiry. I'd be happy to help out–I'm having trouble opening the document on my Mac though, I think there may be an issue with the Chinese character font? I think if you sent me a Word version that might be easiest, as it would also allow me to make comments in the document."*

A few days later the Cheng Li imposter wrote back with a polite message apologizing for the delay in replying and noting he still had to prepare his report on self immolations so there was time for Lhadon to send him comments. The email included a link to a report that was in fact directed towards a website that would serve the visitor malware for windows or a Mac depending on the computer they were using. This response led Lhadon and the Citizen Lab researchers to conclude that the attackers had taken the bait they left in her message.

Lhadon's response included that she was using a Mac, and they likely spent the next four days putting together malware that could infect Mac computers. This digital espionage attempt stood out for the social engineering used to convincingly masquerade as Cheng Li and the technical adaptations the attackers made in real time in hopes of getting access to Lhadon's communications and data.

While tricking the attackers was an empowering moment, overall the experience left an emotional toll on Lhadon.

> *"The attack left me reeling, shattering my sense of security and trust in my online interactions. It amplified my feelings of vulnerability and paranoia. Considering the confidential nature of my*

14. Communities @ Risk: Targeted Digital Threats Against Civil Society", Citizen Lab, November 11, 2014

> *work, the breach threatened to compromise sensitive information, adding another layer of anxiety to my already demanding role."*

SPYING ON THE TIBETAN MOVEMENT DURING COVID

Digital espionage campaigns often take advantage of targeted communities when they are the most vulnerable such as periods of emergency. The COVID pandemic provided a perfect environment for digital espionage operators to spread a different type of infection.

Like the rest of the world the COVID pandemic hit the Tibetan community in early 2020. Tibetans in India were particularly vulnerable due to the lack of access to health services and equipment. Furthermore, the close proximity of the community made self isolation difficult. While dealing with the daily challenges of the pandemic, Tibetans also found themselves under attack from digital espionage campaigns that leveraged concerns over COVID to spread malicious emails.

Emails posing as Tibetan human rights groups included PowerPoint files claiming to offer tips on China's effective management of the COVID-19 outbreak, but these files were actually embedded with malware.

A few months later another espionage email campaign started that spoofed the account of Delek Hospital, one of the main healthcare institutions for the community. The emails included a document with information on "Public Protection against Covid-19". However, again this was a trick and the document was malware designed to spy on the community.

Another COVID-19 theme based email attack was observed where the attackers presented themselves as "DIIR INFO Secretary". Although the content of the email was presented to look like a general public awareness message on Covid-19 from the World Health Organisation (WHO), the interesting fact here is that the email sender information is depicted as the Department of Information and International Relations (DIIR), an executive branch under the CTA. This guidance document was initially published on March 7, 2020, while the weaponized attachment was delivered by threat actors on March 16, 2020. This malicious attachment was later found to exploit a microsoft vulnerability and the malware was later dubbed as 'Sepulcher' by Proofpoint, an american cybersecurity company. They also attributed the Chinese APT group TA413 as the threat actor behind the malicious campaign.[15]

A SPECTRUM OF THREATS

This section provides an overview of the digital threats faced by Tibetan organizations, highlighting how these tactics have adapted and grown more sophisticated over time.

15 Chinese APT TA413 Resumes Targeting of Tibet Following COVID-19 Themed Economic Espionage Campaign Delivering Sepulcher Malware Targeting Europe

IMPERSONATION AND TRUST

Digital espionage against the community often impersonates known people and groups by sending messages and emails that appear to come from trusted sources. Through these impersonations malware can spread through the community and undermine the credibility of Tibetan groups.

The Tibetan Women's Association (TWA) is a key group in the Tibet movement that originates in the courageous protests of Tibetan women against the illegal occupation of Tibet by China in 1959. Targeted digital espionage campaigns have impersonated TWA to send malicious messages to other groups for years.

- In December 2018, a malicious email, purportedly from the TWA, circulated within the community. The email included a malicious attachment titled 'Tibet was never a part of China'. Clicking on the attachment would infect the target's computer with malware capable of extracting sensitive information.

- Similarly, in 2021, another impersonated email, titled 'Inside Tibet and from the Tibetan exile community', targeted institutions like the Library of Tibetan Works and Archive and offices of the Central Tibetan Administration (CTA) abroad. For victims using Firefox browser with Gmail logged in, clicking the malicious link grants near-total access to their Gmail accounts.

These impersonation attacks not only exploit the trust and reputation of Tibetan institutions but also undermine the collective security of the Tibetan community.

Kelsang Dolma, the VicePresident of the TWA recounts the impact the incident had on the group.

"This incident caused us a lot of concern not only on the individual level but also on an organizational level. As an activist association, such impersonation and intrusion attempts to our important files and financial accounts will jeopardize the credibility and trustworthiness of our association within our society."
- Kalsang Dolma (Vice President, Tibetan Women Association)

Responding to the threat, the TWA promptly alerted recipients of the malicious emails to report them and refrain from clicking on any links or attachments. Additionally, TibCERT proactively reached out to organizations that received similar emails, urging them to assess their systems and networks for potential compromise.

POISONING THE WELL: USING TIBETAN WEBSITES AGAINST THE COMMUNITY

Targeted malware is not only delivered through emails or messages. It can also spread through the community by infecting trusted websites. Like a village well, websites for Tibetan media and organizations serve as vital resources for the community. If you poison the well, you poison the village. A "watering hole attack" describes this type of action online. Attackers get unauthorized access to websites and infect them with malware. When users visit the website they are at risk of their computer being infected by the malware and giving access to the attackers. The modus operandi of these attacks is particularly insidious, as compromised websites automatically download malware onto visitors' devices without their knowledge. This method bypasses the need for attackers to target individuals individually, streamlining the process, and maximizing the impact.

Tibetan media and organizational websites, including those of the CTA and the Office of His Holiness the Dalai Lama (OHHDL), have been frequent targets.[16] Community resource websites have also fallen victim including Tibetan Homes Foundation, and a Tibetan school in the diaspora.

Many Tibetan websites have experienced watering hole attacks including media sites and official websites for key organizations such as the CTA and the OHHDL. Community resource websites have also fallen victim including Tibetan Homes Foundation, and a Tibetan school in the diaspora.

Tibet Times started as a Tibetan-language newspaper before evolving into a comprehensive media outlet, offering a Tibetan-language website and a mobile app to disseminate accurate information and breaking news about Tibet. In 2013, a scan for malicious behavior on the TibetTimes website revealed a disturbing discovery: visitors to the site unwittingly opened a malicious domain, potentially exposing their devices to malware.

"When this kind of attack happens to us, it not only tarnishes the credibility of Tibet Times among our viewers but more importantly it jeopardizes their safety as well through potential device infections. Naturally it also creates a worrisome and annoying situation in our working process."

- Tenzin Rabyang(Managing Director, Tibet Times)

Websites like TibetTimes that publish news on human rights violations in Tibet and provide coverage in TIbetan, English and Chinese, attract visitors from both inside Tibet and worldwide. However, these attacks harm the credibility and integrity of TibetTimes while also endangering website visitors. For individuals from Tibet, such attacks could have serious consequences as individuals found accessing or sharing content deemed sensitive by the PRC routinely face harassment, surveillance, or even legal repercussions.

16 Holy Water: Ongoing Targeted Watering-Hole Attack in Asia", Securelist by Kaspersky, March 21, 2020

DIGITAL ATTACKS AS CENSORSHIP

Targeted digital espionage is not the only threat that Tibetan groups experience. Some digital attacks are aimed at blatantly silencing groups through attacks on websites.

Voice of Tibet (VOT) is an independent radio station founded in 1996 with a mission to transmit news to Tibetans inside Tibet and around the world. Tibetan exile media like VOT present a clear threat to China's censorship regime by providing independent news to Tibetans inside Tibet in both Tibetan and Mandarin. The VOT website is blocked in China and its transmissions online and over the air comes under constant threat.

In 2011, VOT experienced massive disruptions of its website and radio signal. The website was taken offline by a Distributed Denial of Service (DDoS) attack overwhelming the website with too much traffic. This type of digital threat works by flooding a website with more requests than it can handle resulting in poor performance or even complete crashes. It's like shutting down a road by causing a massive traffic jam. At the same time as the DDoS attack, VOT's shortwave radio transmissions into Tibet experienced persistent jamming attempts.

A staff at VOT felt it was clear that they were attacked by agents of China in an attempt to silence the service. Oystein Alme, then the project manager at VOT, remarked: "We have noted a significant increase in jamming since 16 March, especially in the cities where the government has invested tens of millions of dollars to install antennae to prevent Tibetans from listening to us."[17]

Tenzin Peldon, Chief Editor at VOT, emphasized the resilience of Tibetan media in the face of adversity, acknowledging the ongoing battle against Chinese censorship. Despite relentless attempts to disrupt their broadcasts,[18] Peldon affirmed VOT's commitment to circumventing censorship through innovative programming strategies. However, the repercussions of these attacks extended beyond VOT, impacting the broader Tibetan community's access to vital information and cultural preservation efforts.[19]

"We were not able to reach our audience on time since our job was to get the news and information to the Tibetans inside Tibet right on time. We couldn't do that for several days because of the attack and I felt that all of our efforts had been wasted."

- Peldon la, (Editor-in-Chief, Voice of Tibet)

Websites served as more than just information hubs; they were vital platforms for cultural preservation, community building, and political advocacy. Threats like DDoS attacks disrupt the flow of information and impede the community's ability to raise awareness about human rights violations in Tibet. Other Tibetan media and civil society groups including Tibet Times, Phayul, and the Tibetan Center for Human Rights and Democracy (TCHRD), also faced similar assaults, highlighting the systematic targeting of Tibetan voices by malicious actors. As Tibetans continue to navigate the

17 "Radio Stations Jammed, Websites, Hacked, Media Restrained in Tibet", Human Rights House Foundation, April 24, 2008

18 Radio Stations Jammed, Websites, Hacked, Media Restrained in Tibet", Human Rights House Foundation, April 24, 2008

19 The High-Tech War on Tibetan Communication", Engadget, June 27, 2017

digital landscape, safeguarding their online platforms becomes paramount to upholding their right to free expression and preserving their cultural heritage.

THE SPY IN YOUR POCKET

In the early 2010s, the rise of smartphones introduced new opportunities for connectivity for the Tibetan community. The ubiquity of mobile technology connected Tibetans in Tibet and the diaspora in ways that had not been experienced before. Reports from inside became available as events happened. Families separated by exile went from periodic updates to daily communications. But as this new connectivity flourished espionage threats went mobile as well.

MOBILE THREATS EMERGE

In 2011, WeChat, a mobile messaging application, launched and has become the most popular communications platform in China and quickly spread to Tibetan populations. The popularity of WeChat became a concern due to the app being under the control of a Chinese company and therefore subject to information controls dictated by the Chinese government. Reports of censorship and suspected surveillance on WeChat began to circulate in the community

Tibet Action Institute is an activist organization that uses digital technology and strategic nonviolent action to support the Tibet movement. In response to digital security concerns surrounding WeChat, Tibet Action Institute promoted alternative communications apps to Tibetans including KakaoTalk (a South Korean chat app).

Lobsang Gyatso Sither, then serving as the Digital Security Program Manager at Tibet Action Institute promoted this campaign by sending trusted contacts installation files for the apps on Android (Android Application Package File, APKs).

On December 4, 2012, Lobsang sent an email to a member of the Tibetan Parliament that included APKs for KakaoTalk and Internet radio apps with instructions on how to install and use the apps.

On January 16, 2013, a high profile member of the Tibetan community received an identical email that appeared to also come from Lobsang. This email was a fake and attached APK files with additional features that were designed to send a user's contacts, SMS message history, and cellular network location to attackers.[20]

This chain of events suggests that the email of the Tibetan Parliamentarian who first received the real email was already compromised, giving the attackers access to the message and showing them that Tibetans were circulating APKs through their networks of trust. The attackers then repurposed the message and modified the APKs to include malware.

20 "Permission to Spy: An Analysis of Android Malware Targeting Tibetans", Citizen Lab, April 18, 2013

"As someone working on digital security and constantly looking at phishing attacks, it was a surprise to see your own email being used for phishing purposes and I wasn't sure how to feel about it. Once I learned more about the attack, the fact that I had no idea how many people might have been lured with this email was scary. Also, how something that is meant for allowing people to access information has been repurposed by the Chinese Government to spy on them made me angry. It also made me realize the truth that Tibetans are targeted as a community and our response has to be community led".

- Lobsang Gyatso Sither (Director of Technology,Tibet Action Institute)

This attack was one of the first examples of mobile malware we observed in the community and showed how digital threats against the community adapt. As Tibetans went mobile, so did the threats.

ONE CLICK AWAY FROM COMPROMISE

"Considering the work we do, which directly revolves around exposing China for its various forms of human rights abuses in Tibet, and also because similar viruses I've received [have targeted] other Tibetan activist groups working on the issue, it is clear it is a work of the Chinese Communist government."[21]

- Lhagyari Namgyal Dolkar (Activist and Member of Tibetan Parliament in Exile)

The sophistication of social engineering used to lure targets to install mobile malware and the technical sophistication of the malware itself has significantly escalated in recent years.

Between November 2018 and May 2019, senior members of key Tibetan groups received malicious links in individually tailored WhatsApp text messages made to appear to be from NGO workers, journalists, and other fake personas. The links led to code designed to exploit web browser vulnerabilities to install spyware on iOS and Android devices. This kind of threat is called a "one click exploit", because all it takes is one click of a link for a target to be compromised. This espionage campaign is one of the most sophisticated we have observed in the community over the last decade.

Among the targets of this campaign was Namgyal Dolkar, a Tibetan parliamentarian. On the night of November 12, 2018, she received a WhatsApp message from "Jason Wu" who claimed to be the head of the Refugee Group at Amnesty International's Hong Kong branch. Namgyal Dolkar often receives unsolicited messages from human rights organizations seeking her assistance so this message did not seem out of the ordinary. She replied to "Jason" who proceeded to describe a recent self-immolation in Tibet, asked her to help verify the incident for an upcoming Amnesty International report on human rights in China, and sent a link. Namgyal Dolkar forwarded the message to TibCERT who in collaboration with researchers at the Citizen Lab discovered the link connected to exploits designed

21 "Android and iPhones Hacked with Just One WhatsApp Click - and Tibetans are Under Assault", Central Tibetan Administration, September 25, 2019

to infect iPhone and Android devices with malware.[22]

Amnesty International does not employ anyone named Jason Wu. The message was very carefully crafted to trick Namgyal Dolkar into clicking the link, which would infect her phone with malware. For Namgyal Dolkar, the real sender of the message was clear. She firmly suspects China behind the campaign as China has long persecuted the Tibetan freedom movement in exile.

In total, we found 17 high profile members of the Tibetan community who were targeted by the same campaign including members of the Offices of His Holiness the Dalai Lama, the Central Tibet Administration, Tibetan Parliamentarians and Tibetan human rights groups. This campaign was highly organized and targeted with multiple fake personas used. In every case the fake persona engaged the target in a conversation and once an exchange had started would send a malicious link. All it would take is one click of the link for the target's phone to be turned into a spy in their pocket.

22 Tibetan Targeted by Spyware for iPhone and Android", TibCERT, September 24, 2019 (https://citizenlab.ca/..) (https://blog.tibcert.org/...)

THE COMMUNITY RESPONDS

From the moment the Tibetan community came online it has faced persistent digital espionage. Over decades of being targeted, the community has grown capacities and resilience for defending against digital threats.

A key mission of Tibet Action institute is to defend against relentless cyber attacks and surveillance from China. Since its inception, the group has led campaigns for digital security awareness and training.[1] Efforts include digital security education campaigns focused on fundamental topics such as basic web browser security and how to prevent malware infection. These campaigns feature references to Tibetan culture such as the Detach from Attachments campaign that drew on Buddhist teachings to impart a similar message: [2]

This type of behavior change can be an effective way to defend against targeted digital espionage. A study from the Citizen Lab found that in the early 2010s malicious file attachments were the most common threat Tibetan organizations received. The researchers found that simply not opening email attachments would have prevented over 95 percent of the threats the Tibetan groups in the study received.[3] These findings show that education is an essential foundation for increasing digital security defense. However, there is an inherent asymmetry between the digital defenses of Tibetan groups and the capabilities of the operators who target them.

State sponsored espionage operators have exponentially more resources to develop and conduct digital espionage than civil society has to defend themselves. As our review of digital espionage shows, threats evolve over time and are quick to adapt to changes in how the community uses technology and implements defenses. Changing the behavior of a community is a slow and gradual process, while an adversary can evolve overnight. Therefore, while education and training are essential efforts that must continue, more was needed to sufficiently respond to the threat including a platform through which Tibetans themselves could enact their own cyberdefense instead of relying solely on outside support and through this platform elevate the skills of community members to provide this protection.

The Tibetan Computer Emergency Readiness Team or TibCERT[4] was started in November 2018 as a program of Tibet Action Institute as a way to combat the threats that Tibetans have faced and continue to face. TibCERT was a natural progression to the digital security work that Tibet Action Institute had been carrying out in the community for over a decade. It was about bringing all the stakeholders together and building a community wide response.

---

1 https://tibetaction.net/digitalsecurity/

2 "Detach from Attachments", Tibet Action Institute, 2012 https://vimeo.com/32992617

3 "Targeted Threat Index: Characterizing and Quantifying Politically-Motivated Targeted Malware", Usenix, August 20-22, 2014

4 Tibetan Computer Readiness Team (TibCERT) https://tibcert.org/

TibCERT follows the standard model for CERTS (Computer Emergency Response Teams) which are expert groups that handle computer security incidents. Countries have government run CERTS that operate on the national level tasked with protecting their country from digital threats. There are also sector level CERTS that facilitate threat intelligence sharing between companies in specific areas such as finance. TibCERT operates in this model to provide threat intelligence sharing, incident response, and technical support to Tibetan member organizations. TibCERT includes two main programs. TibCERT Recon focuses investigating threats facing Tibetans in exile and surveillance within Tibet, including this report. TibCERT Response facilitates knowledge sharing and collaborative threat mitigation among stakeholders. Forming a professionalized Computer Emergency Readiness Team for the Tibetan community represents a significant milestone in developing robust resilience to digital threats.

Lobsang Gyatso Sither, one of the founders of TibCERT, reflects on the motivations to start the group.

"There were a number of reasons why TibCERT was formed. It came from discussions internally with Nathan Frietas (co-founder of Tibet Action Institute) and the rest of the digital security team as well as with partners at the Citizen Lab about how the Tibetan community in the diaspora has been targeted with spyware as a community and any solution that we develop must be community led.

At the same time, there was another reason which was about taking the online CERT space back for Tibet so that TibCERT is an entity responsible for protecting the digital space for both Tibetans inside Tibet and outside Tibet. Our goal is to build internal capacity and also standardize the structure of this community led initiative so that it can partner with global researchers on shared protocols."

- Lobsang Gyatso Sither (Director of Technology,Tibet Action Institute)

To extend its reach, TibCERT has deployed Digital Security Ambassadors in major settlements in India, providing technical assistance and incident response to local communities. Additionally, TibCERT has initiated the TibCERT Response Hub Program, establishing incident response hubs in Dharamshala, Mundgod, and Bylakuppe, where volunteers convene monthly to address community-specific challenges and implement solutions. In 2022, two of the TibCERT Response Hubs based in South India were converted to TibCERT Community Centers by expanding its objectives by providing digital security resources for the entire community and providing a space for engagement with the entire community particularly within monastic institutions.

Currently encompassing over 50 organizations and institutions, TibCERT currently offers incident response services and assisting in the development & implementation of digital security policies. These efforts aim to foster a secure work environment and fortify the overall digital resilience of Tibetan individuals and organizations within the community and beyond.

The primary goal of this report is to empower Tibetans by fostering a sense of ownership and pride in confronting cyberattacks with unity and innovation. While the Tibetan community has made significant strides in coming together to address unprecedented digital threats and sustain the freedom movement in the digital age, it still requires substantial support and collaboration from global and security experts. The necessity of prioritizing digital security stems from decades of being targeted by government-sponsored espionage. However, Tibetans are not only ones facing such challenges - these threats extend to civil society globally.

Numerous investigations have revealed that the sponsors and operators of these operations often share common tactics, techniques, and procedures. This makes it crucial for civil society as a whole to adopt a similar approach, coordinating efforts to exchange knowledge and data about threats while sharing best practices for defense. Given the shared experiences of civil society groups worldwide in confronting information security challenges, a collective strategy may lead to more substantial results than tackling these threats in isolation.

Another goal of sharing the first hand experiences of Tibetans targeted by digital espionage and how our community responds to this challenge is informing and providing inspirations to other human rights groups who may just be becoming aware of digital espionage.

The Tibetan community must continue to work together to maintain resilience to digital espionage and the long reach of China. We also must stand in solidarity with civil society groups around the world that are facing transnational repression from authoritarian regimes. Together we can empower each other and form a more secure, free, and open Internet that enables movements to create positive social change.

This report in its entirety aims to put a face to these attacks and underscores how these attacks impact real people and at the same time, how community led initiatives are key towards building resilience.