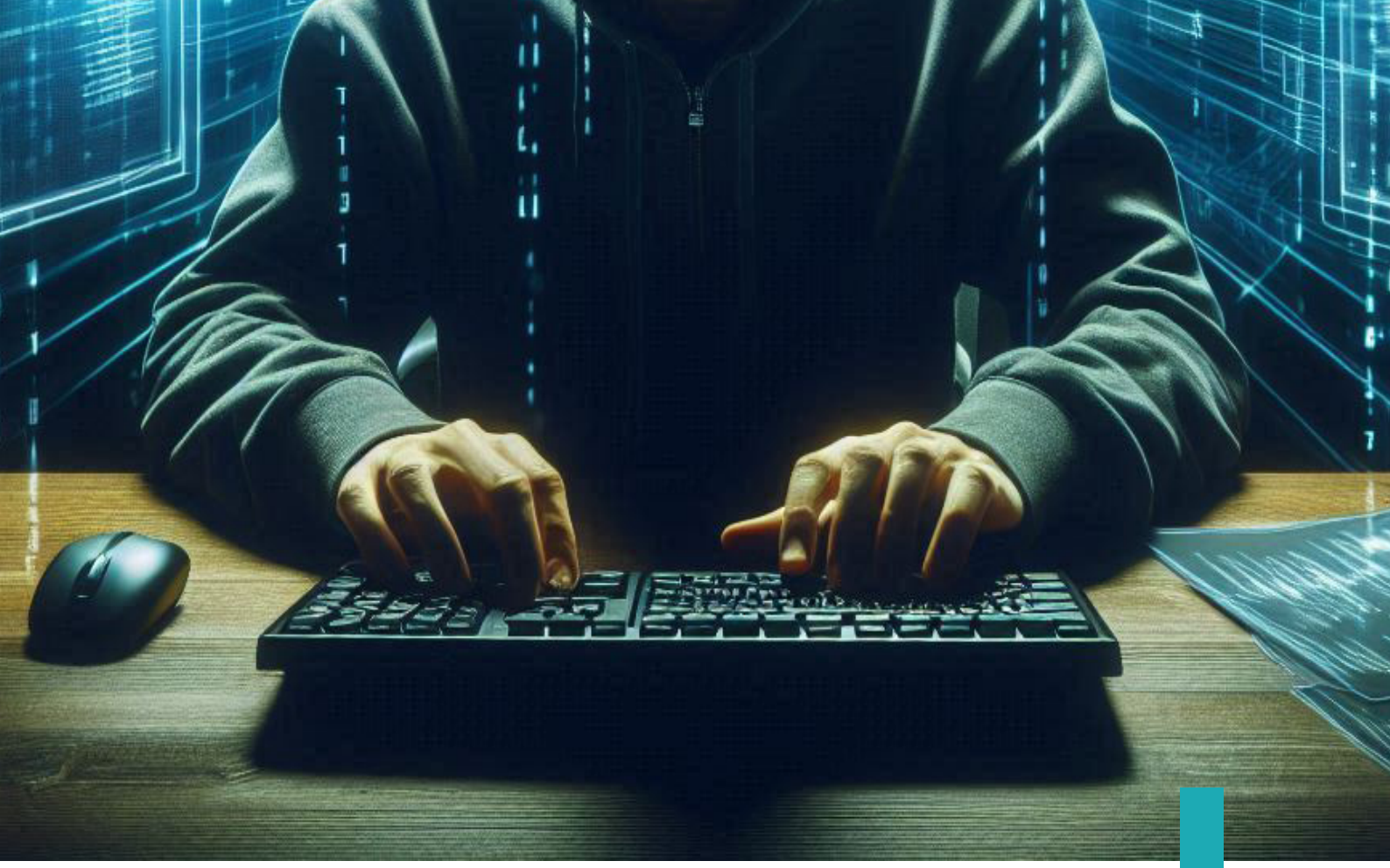

CYBER ESPIONAGE AGAINST TIBETANS:

AN ANALYSIS OF OVER TWO DECADES OF PUBLICLY AVAILABLE DATA

TIBCERT

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

Tibet Action Institute
བོད་ཀྱི་ལས་འགུལ་བསྟི་གནས་ཁང་།

CONTENTS

SUMMARY

The emergence and proliferation of information technology in the Tibetan community in exile has been integral for strengthening the Tibetan movement, expanding communication opportunities, and providing information on Tibetan culture. However, as infrastructure, tools, and knowledge spread through the community, so do online threats perpetrated by groups tied to the Chinese Communist Party (CCP). These groups take advantage of relatively low levels of information security capacity in the Tibetan community to infiltrate the communications and monitor groups and individuals.

This report provides an overview of the past 20 years of information security threats targeting the Tibetan community based on analysis of publicly available research reports and testimonies from targeted individuals. The report also highlights initiatives led by Tibet Action Institute towards mitigating these threats through hyper-localized public awareness campaigns and the establishment of TibCERT - a diaspora based collaborative computer emergency readiness team(CERT)[1] model approach to prevent and mitigate online threats against the Tibetan community.

The report provides a technical overview of the threats, analysis of the possible intention behind the, how these threats evolve over time, and concludes with recommendations for strengthening community defense and resilience.

EARLY INTERNET DEVELOPMENT IN THE TIBETAN DIASPORA

Understanding the information threats targeting the Tibetan diaspora requires situating these threats in the history of how the community first came online. The period of 1995-1996 was a crucial moment when Tibetans in the diaspora were able to leverage the network infrastructure that made the Internet accessible to the Offices of His Holiness the Dalai Lama (OHHDL) and the Tibetan Government in Exile (TGiE) thanks to a dedicated team of volunteers. This connectivity amplified the reach of the Tibetan movement but also opened it up to online threats.

1 Computer Emergency Response Team (CERT)

The World Wide Web emerged in India in the 1990s when the computer literacy of the Tibetan diaspora was still in its infancy. Before 1995, the World Wide Web was only known by a few Tibetans and long distance communications were done through fax machines. Long distance calls were expensive and telephone lines were unreliable. Before 1995, the 200 staff of the TGiE had to physically transfer data between computers. Without a network, writing an email was an arduous process that required typing out text on a computer, storing the data on a disk and walking 2 kilometers to transfer the data to the next computer. The 2 km walk just to send data led to people from abroad calling the foot powered infrastructure the "Sneaker net". A group from Silicon Valley consisting of five computer experts came to revolutionize the outdated sneaker network to a modernized email and web infrastructure for the TGiE. The idea evolved from Web architect Dan Haig who with his companions, Webmaster Stefan Lisowski, Web designer Ari Salomon, and computer specialist Jack Burris were determined to revolutionize the Internet infrastructure for the TGiE.[2] The idea evolved from Web architect Dan Haig who with his companions, Webmaster Stefan Lisowski, Web designer Ari Salomon, and computer specialist Jack Burris were determined to revolutionize the Internet infrastructure for the TGiE.

Dan Haig visited India in 1995 after quitting his job at the tech website CNET in San Francisco to attend a series of lectures at the Men-Tsee-Khang Institute (Tibetan Medical and Astro Institute) in Dharamsala. Dharamshala is a hub of many prominent Tibetan institutions, civil society organizations and l public figures working for the Tibetan movement. Just before Dan Haig left India, he met Phuntsok Namgyal, the then Director of the Tibetan Computer Resource Center (TCRC, the computer support center for the TGiE) who presented to him a project called "The Tibetan Global Link," which sought to improve and enhance the digital and Internet infrastructure connecting major offices and institutions within the diaspora community in Dharamsala. Dan Haig agreed to assist with the project and contribute his time and expertise. About a year and a half after this initial visit Dan Haig and a team of volunteers came to Dharamsala to revamp and revolutionize the Internet and network infrastructure.

The project was an intense challenge to support and implement. It required $60,000 US in materials including computers, modems, enormous drills, and hundreds of meters of steel and coaxial cable. Setting up this infrastructure took 18 months of dangerous work including drilling and climbing precarious roofs amidst constant power failures and persistent rain from an early monsoon season.

2 High Tech for the Dalai Lama

Once the network was established in 1996, a new "Email culture" developed, email users in the community rose exponentially, and a new web domain "www.tibet.com" became the online face of Tibetan movement in exile. This official website of TGiE evolved along the years to CTA's current site, www.tibet.net that is used today.

This wave of Internet development was a crucial moment that made information on Tibet more accessible and increased the reach of the Tibetan movement. During this period, the works and updates of His Holiness the Dalai Lama were made available online. Monks began managing office email, maintaining databases, and hosting a comprehensive website with a wide range of services and sources of information. The meetings of the Dalai Lama with international diplomats and religious leaders around the world were scheduled via email through the Office of His Holiness The Dalai Lama (OHHDL).

The momentum the Tibetan movement received from connecting to the world through the Internet was undoubtedly a concern for the CCP. While the new connectivity brought the Tibetan community many benefits, the overall security level of networks and computers was low. This vulnerability was exploited by hacker groups connected to the CCP. At these early stages malware attacks against the community have been documented including incidents such as confidential emails from OHHDL being intercepted by CCP agencies who further attempted to put diplomatic pressure on those who should be responding to email communications from OHHDL.[3]

On September 27, 2002, Jigme Tsering, the head of TCRC issued a statement detailing Chinese attempts to infiltrate computers of the Tibetan Government In Exile. He mentioned:[4]

> "A number of targeted computer viruses circulating via email throughout the Tibetan Government-in-exile and Tibetan support groups and related NGOs 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 off an infected computer and send it via email to an address in Beijing."

3 The snooping dragon: social-malware surveillance of the Tibetan movement
4 Chinese Internet group found spying on Tibetan government computers

Attempts to infiltrate the networks and communications of the Tibetan community have persisted to this day. Over the past 20 years these attacks have been well documented by researchers in academia and the private sector. Reviewing this literature provides a history of information security threats against the community. This report is based on an analysis of public reports available on targeted attacks against the Tibetan community.

METHODOLOGY

This report is based on an analysis of public reports available on targeted attacks against the Tibetan community. It is also an outcome of various analyses and experiences associated with TibCERT's incident response support to various organizations, institutions and individuals within the Tibetan diaspora community in India. The report documents testimonies and interviews from people in the Tibetan diaspora community who have been targeted by cyber espionage to understand the timeline, impact and the potential motive behind those attacks.

We selected reports to review based on references to attacks on the Tibetan diaspora. The public reports are authored by information security companies and academic groups including: Citizen Lab (University of Toronto), Kaspersky, Trend Micro, Palo Alto Networks , AT&T Alien Labs, Proofpoint, Recorded Future, and Security Week.

We collected 63 reports and categorized them on the basis of the following details:

- Report publication date
- Organization or firm who published the report
- The title of the report
- Incident start and end dates if mentioned
- The attack vector through which incident took place
- CVE of the malware
- Malware associated with the incident
- The platform on which incident took place
- Name of the Threat Actor or the Campaign associated with it

Identifying the incident start and end date mentioned in these reports and comparing those with the report publication date helped us to build a timeline of information threat incidents against the community. Our analysis of technical details referenced in the reports was focused on reviewing the level of effort put in these attacks, tactics used by these attackers, evolution of threats over time, and what inferences we can make to understand who these threat actors are and their

motivations for carrying out the attacks.

TibCERT's experience of providing incident response to Tibetan institutions and organizations within the diaspora provides perspective into the wave of targeted digital espionage that persistently tries to infiltrate and subvert the Tibetan movement. Spoofed malicious email attacks circulated within the community in the past years have shown us how these threat actors masquerade as existing legitimate organizations causing a great concern and confusion as to which emails are legitimate and which ones are malicious.

We interviewed people who were active in the early phases of Internet infrastructure development within the Tibetan community through a series of questions focused on the ground level experience they had in these cyber attack scenarios at the time. Their personal testimonies in relation to these targeted attacks offer us a basic understanding of how they were victimized by these cyber attacks, what difficulties it put them through and in what ways they tried to cope up with these digital security difficulties at the time. Information from these interviews helped us document key facts and perspectives from the community itself, which cannot be found through a review of public threat intelligence reports.

THREAT TRENDS AGAINST THE TIBETAN COMMUNITY

OUR ANALYSIS OF PUBLIC INFORMATION SECURITY REPORTS REVEALS A NUMBER OF TRENDS IN DIGITAL THREATS AGAINST THE TIBETAN COMMUNITY.

INFORMATION THREATS AGAINST THE TIBETAN COMMUNITY ARE A FORM OF POLITICAL ESPIONAGE

The ultimate goal of cyber attacks against the Tibetan community is infiltrating communications and collecting information for political advantage. This form of espionage has been a threat since the early development of the Internet in the community. Relentless cyber attacks were observed throughout the past 20 years which were found to infect and infiltrate the computers in the Office Of His Holiness The Dalai Lama (OHHDL), Central Tibetan Administration (CTA), Tibetan Non-

Governmental/Non-Profit Organizations (NGOs) and other prominent figures which include ex-diplomats, activists and journalists etc.

The first major published reports by security researchers regarding the targeted cyber attack against the Tibetan diaspora community appeared from 2009 onwards, including Tracking Ghostnet and Shadow In The Clouds published by the Information Warfare Monitor. However tracing back the origins of the first internet infrastructure developed in the diaspora and following testimonies and anecdotal evidence of past victims reveals earlier incidents. The first series of cyber attack against the community was reported by Jigmey Tsering, (Manager of the Tibetan Computer Resource Center at the time) who alleged that in between 1999 and 2001, their office was targeted by suspicious emails posing as if they were coming from OHHDL, which included malware implanted attachments capable of lifting confidential files from PCs used by the center. Jigmey Tsering notes that these virus-infected emails were traced back to six different addresses in China. The first known such incidents documented and published online were reported by John Leyden, an independent cybersecurity journalist on April 29, 2002[5] and by the International Campaign for Tibet on October 28, 2003.[6] These attacks involved malicious emails crafted to impersonate trusted figures and organizations, such as TGiE officials and Tibet advocacy groups, exploiting key events like the Fourth International Tibet Support Group Conference. The emails contained attachments—Trojan horse malware—that, when opened, compromised devices, extracted sensitive data, and transmitted it back to Chinese-controlled networks. Evidence linked these operations to Beijing-based IP addresses and government-controlled networks, highlighting their strategic intent. The malware used was highly customized to exploit community vulnerabilities, illustrating an early, calculated use of cyber tools to undermine the Tibetan movement's digital and operational security.

In 2009, the Information Warfare Monitor published Tracking GhostNet, a report that uncovered a cyber espionage operation that compromised high level Tibetan organizations including the Private Office of His Holiness the Dalai Lama as well as government offices in 103 countries. At the time there were very few public reports of targeted malware campaigns and GhostNet was the first major digital espionage campaign targeting the Tibetan community that was brought to public attention. Server infrastructure used by GhostNet was tracked to locations in China and the targets could all be interpreted as being geopolitical interests of the Chinese government. However, beyond these findings the report did not make a conclusive connection between the GhostNet and the CCP. Nonetheless what is evident is that

5 Chinese Internet group found spying on Tibetan government computers
6 Chinese Internet group found spying on Tibetan government computers

the objective of the operation was political espionage and the Tibetan community was a focal point.

A follow-up report, Shadows in the Cloud, published by the Information Warfare Monitor in 2010, found that a similar operation stole sensitive information from the OHHDL including thousands of email addresses and details of the Dalai Lama's envoy's negotiating positions.

The impact of digital espionage in the form of remote surveillance and stealing critical information from unsuspecting victims has been documented in the report, such as the Drewla incident. Drewla ('connection' in Tibetan) was an online outreach project was set up in 2005 that employed Tibetan youth with Chinese language skills to chat with people in mainland China and in the diaspora, raising awareness about the Tibetan situation, sharing the teachings of His Holiness the Dalai Lama, and supplying information on how to circumvent Chinese government censorship on the Internet. A Drewla computer was found to be compromised by GhostNet on September 12, 2008 and consequently a member of Drewla, a young woman was arrested[7] at the Nepalese-Tibetan border where Chinese intelligence personnel presented her with full transcripts of her Internet chats over the years. They also indicated that they were monitoring the "Drewla outreach initiative" and that her colleagues were not welcome to return to Tibet.

THE TIBETAN COMMUNITY IS TARGETED AS A COMMUNITY

The Tibetan community is targeted as a community with individuals and various groups often experiencing the same attacks. Much of this threat activity is centered on Dharamsala, India, which is the permanent residence of His Holiness the Dalai Lama ever since his escape into exile and is also the base for the Tibetan Government In Exile, now known as Central Tibetan Administration.

A majority of cyber attacks against the community leveraged on similar tactics, techniques and procedures in the form of malicious emails that which were circulated masquerading as legitimate Tibetan organizations, Human rights support groups and individuals around the world. Numerous DDoS and watering hole attacks were observed around similar timelines on official sites of OHHDL, CTA and NGOs. These attacks are targeted to either disrupt the flow of information from these sites or to exploit and manipulate the trust that the end users have in

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

visiting these popular sites so as to eventually infect or gather details of website visitors.

Of the public reports we reviewed that reference the Tibetan community as targets, a number of them pinpoint specific types of groups in the community. The most frequently cited targets are Tibetan NGOs such as Tibetan Women Association, Tibetan Centre for Human Rights and Democracy, Students for a Free Tibet, followed by CTA , media groups and Activists (individuals). Of the 63 reports we reviewed, 30 reports mention NGO groups, 14 reports mention Tibetan activists, 13 reports mention CTA and 6 reports mention media groups.

S.No	Group	Percentage	Number of incidents
1	NGO	51%	30
2	Tibetan Activists	24%	14
3	CTA	22%	13
4	Media groups	10%	6

MOST TARGETED VICTIMS IN THE TIBETAN DIASPORA

Fig 1. Most targeted victims of cyber attacks against the Tibetan diaspora.

TECHNICAL SOPHISTICATION OF THE ATTACKS IS LOW, BUT SOCIAL ENGINEERING IS ADVANCED

Malware attacks against the community typically use outdated software exploits and basic remote access trojans. While the technical sophistication is generally low, great effort is put into social engineering tactics designed to lure targets into opening a malicious attachment or link. The social engineering tactics used by attackers demonstrate how compromising one group within the community can lead to a cascading effect, putting other groups at risk. Once an organization's computer is compromised, attackers gain access to sensitive information such as contact lists, event details, information on prominent public figures, and other data. This information is then leveraged to target additional groups, amplifying the scope and impact of the attack.

In 2014 the Citizen Lab developed the Targeted Threat Index, a metric that assesses both social engineering and technical sophistication to evaluate the risk of malware threats. The Citizen Lab applied the index to a collection of targeted malware samples from Tibetan NGOs and found that the technical sophistication of targeted malware delivered to the groups was relatively low (relative to commercial malware that has been found targeting civil society groups and journalists and conventional financially motivated malware), with much more effort given to socially engineering messages to mislead users.

From our observation, we noticed that apart from the malicious observables (links and attachments) associated with the emails, the text body of these malicious emails indicate a carefully crafted social engineering tactic to lure vulnerable victims. A majority of these targeted emails suggest a close connection of incidents that show a correlation to contemporary events and incidents that took place inside Tibet and in the diaspora community. For instance, between 2009-2012, we consistently observed a series of self-immolation themed emails with senders posing as international journalists and staff at Tibet support groups to lure victims into clicking links and attachments. Malicious emails in the past were also themed around political and cultural events held each year within the Tibetan diaspora community such as the March 10th National Uprising Day, 2nd Tibetan Democracy Day on September 2 etc. In addition to these social engineering tactics, attackers also sent emails consisting of a malicious version[8] of an official report titled "Tibet was never a part of China" released by The CTA, just a few months prior to the

8 https://threatpost.com/spy-spam-tibet-exilerat/141460/

malicious email received. In conclusion the threat actors have invested effort in crafting deceptive emails to confuse and lure the unsuspecting victims into clicking such malicious links and attachments.

Common social engineering tactics deployed by these threat actors against the Tibetan diaspora community are as follows :

- Spoofed email sender domains and ID to leverage trust of unassuming victims.
- Carefully crafted email theme
  - Reflecting purpose of the email as per the email receiver.
  - Email theme relevance based on contemporary events/incidents happening inside Tibet and in the diaspora community.
- Choice of victims
  - Organizations, institutions and prominent individuals who share a common goal of advocating the Tibetan movement in exile.
- Name of the Attachment/Link crafted to seem like a genuine public report based on a familiar event, incident or a recently published official report.

Reviewing information on the malware and exploits used in attacks documented in public reports finds similar patterns. Common vulnerability and exposures (CVE) is a reference system used to index publicly reported security vulnerabilities. Out of the more than 50 research reports on threats against the Tibetan community, approximately 37 different CVEs were used in the attacks. The most dangerous type of vulnerabilities are ones where there is no known patch released. These vulnerabilities are called “zero days”, because there has been zero days since a patch has been released. The vulnerabilities exploited in attacks against Tibetans are typically ones that have been known and patched. The top six most prevalent CVEs used are listed below and in Figure TKTK.

- CVE-2012-0158 - 20%
- CVE-2010-3333 - 15%
- CVE-2011-3544 - 8%
- CVE-2012-0507 - 6%
- CVE-2009-3129 - 6%
- CVE-2013-0640 - 6%
- OTHER CVEs - 39%

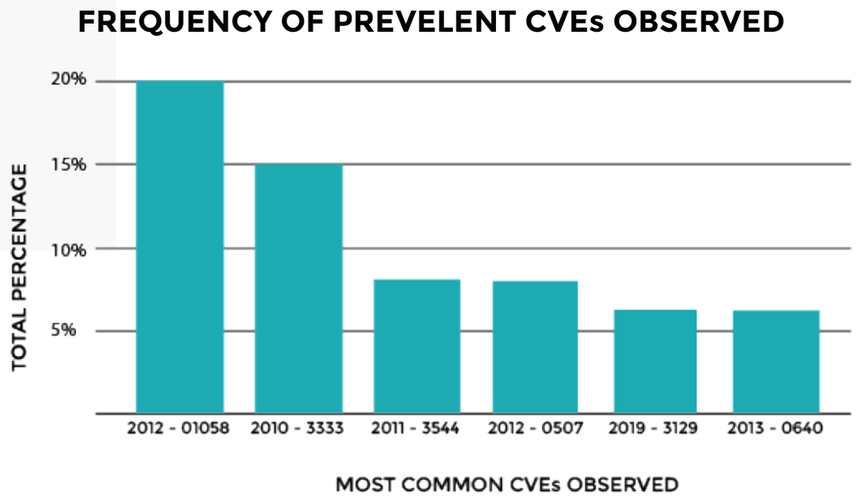

Fig 2. Top 6 commonly used CVEs to infect Tibetan Community with computer/mobile malwares.

The most common exploit used was CVE-2012-0158 which targets a vulnerability in Microsoft Word that was made public in 2012. This vulnerability was subsequently patched soon after the CVE was announced. However, despite the vulnerability being fixed, the exploit continued to be used in malware campaigns in 2013, 2014, 2015, and 2016. The persistent use of this known and patched exploit indicates that the attackers were still likely finding success with it in operations against the community, likely due to victims using unpatched systems and possibly unauthentic versions of Windows.

EMAIL ATTACHMENTS ARE HISTORICALLY THE MOST COMMON ATTACK VECTOR

Throughout the documented incidents the most common attack vector was malicious attachments sent in socially engineered emails representing 60% of the reviewed reports.

This trend was noticed within the community and in response, in 2012, Tibet Action institute promoted a user awareness campaign “Detach from Attachments,” which advised the use of cloud platforms to share documents such as Google Drive or DropBox as an alternative to email attachments. Considering the widespread use of email for both personal and professional purposes, such awareness training could prove highly effective in mitigating risks associated with email attachments. In the Citizen Lab’s Targeted Threat Index research for 2 of the 3 Tibetan organizations in

the study (with at least 40 submitted e-mails), simply not opening attachments would mitigate more than 95% of targeted malware threats that use email as a vector.

Incident Vector	Number of Incident	Percentage
Attachement	35	60%
Phishing	17	29%
Watering Hole	15	25%
Link	10	17%
Google Drive	1	1%
Social Media Message	1	1%

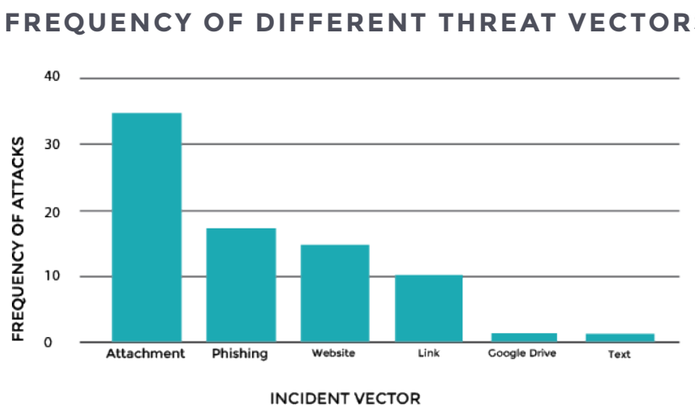

Fig 3. Most commonly used incident vectors out of 58 incidents.

WINDOWS IS HISTORICALLY THE MOST COMMONLY TARGETED PLATFORM.

Throughout the reported incidents, the most commonly targeted platform was Windows, representing 72% of reviewed reports. This finding corresponds with general malware trends and is not surprising given that most of the community works on Windows devices. However, while this is a consistent trend there are also threats targeting Mac OS and mobile platforms.

Incident Platform	Number of incidents	Percentage
Windows	42	72%
Mac	14	24%
Android	7	12%
iSO	3	5%

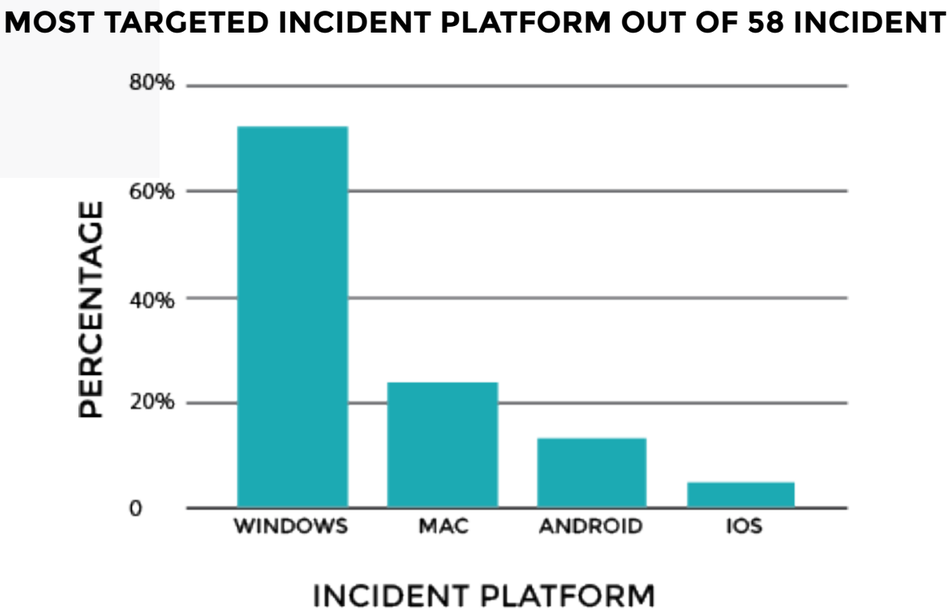

Fig 4. Most targeted incident platforms out of 58 incidents

THREATS ARE EVOLVING

While malicious attachments and malware targeting Windows have historically been the focus of information security threats, the documented incidents also show shifts in tactics seemingly tied to changes in the defensive posture of the community.

Potentially in response to the efforts to encourage users to be more vigilant with email attachments and move to cloud based services, attackers began using Google Drive links to disseminate malware in 2014. As community members were being trained to use Google Drive and trust it more than email attachments, threats shifted to phishing emails designed to collect credentials for Gmail and other email services. The first major reported campaign using this tactic was reported by the Citizen Lab in 2018 and was active from 2016 to 2019. The campaign was technically simple and cheap to set up; it used a server infrastructure that cost an estimated $1,000 US and only required basic system administration and web development skills to maintain. This operation signaled a change in targeting from attempting to infiltrate computer systems to focusing on online services. Phishing is much cheaper than malware

development and the majority of communication, organization, and work happens on email and other platforms which makes compromising them a rich source of information.

Since 2012, many watering hole attacks were observed infecting official sites of CTA and other NGOs as well as people who accessed these infected sites at the time. A Watering hole attack is an information security threat in which the attacker seeks to compromise a specific group of end users by infecting websites with malware that members of the group are known to visit. The goal is to infect a targeted user's computer and gain access to any connected networks. A number of key websites share information and awareness about the Tibetan movement, including the official site of CTA, OHHDL and various NGOs in the diaspora. These websites are frequently visited by Tibetans in Tibet and in exile, and Tibet supporters. These websites are the information equivalent of a village well and if the water is infected eventually the village will be infected? – The Waterhole attacks in a similar way manipulate the overall trust that users have in visiting these popular sites.

The official site of CTA was compromised in 2012 and interestingly only the Chinese language version of the site was infected. The exploit in the Chinese section of the website was found to execute malicious executables to its visitors. There is a high possibility that since the Chinese section of the site is accessed by many Tibetans in Tibet, the act of infecting this section will also indirectly install malicious executables to those Tibetan individuals living in Tibet or China.

While the majority of attacks against the Tibetan community target computer operating systems like Windows or MacOs, we have also seen an emergence of mobile threats. The first instance of mobile malware documented in the community was in 2013. This incident started with a routine email between members in the community. Lobsang Gyatso Sither, presently the Director Of Technology at Tibet Action Institute, sent an email to a Tibetan parliament member that encouraged the use of alternatives to WeChat when communicating with individuals in the Tibetan community. Attached to the email were Kakao Talk (a Korean instant messaging app) and Tunein (an online radio application) as Android .apk files. A month later an email purporting to be Lobsang Gyatso Sither was sent to a high profile political figure in the Tibetan community. It contained the same text as the previous message but attached malicious versions of the same Kakao Talk and Tunein Android APK files. If the malicious versions of these apps were installed, attackers could collect data from infected mobile devices including contacts, call logs, SMS messages, geo-location, and phone data (phone number, OS version, phone model, SDK version). This attack suggests that the Tibetan parliamentarian

that the first genuine message was sent to likely had a compromised computer that allowed the attackers access to the email.

A major escalation in mobile threats targeting the community happened between 2018 to 2019 when a number of prominent figures in the Tibetan community were targeted with malicious links on WhatsApp. The links were to code designed to exploit web browser vulnerabilities to install spyware on iOS and Android devices and would infect users with only one click. This incident marked the first time iOS malware and one click mobile exploits were seen in the community.

Among those targeted by hackers between November 2018 and May 2019 were the offices of the Dalai Lama, the Tibetan Government in Exile, Parliamentarians, and Tibetan NGOs. A total of 17 attempts were made over this period. It is still unclear how the hackers got hold of the targeted individuals, organizations details or contact numbers. The numbers may have been scraped from websites, social media profiles or collected from compromised devices and accounts.

Namgyal Dolkar Lhagyari, a prominent member of the Tibetan exile community received malicious links from a stranger posing as a journalist from Amnesty International in Hong Kong. The sender claimed to be interested in information regarding a self-immolation, a form of protest by Tibetans, and provided a purported news link. Later she contacted TibCERT who in collaboration with the Citizen Lab confirmed that the link pointed to an Android malware. The Citizen Lab called the attack group Poison Carp and found technical links[9] between it and a group revealed by Google Project Zero and Volexity in August 2019 that targeted the Uyghur community with mobile malware.

In 2022, zero day exploits deployed by the threat actor APT TA413 were seen used against the Tibetan diaspora community. The exploit was documented in the report[10] as "A now-patched zero-day vulnerability targeting the Sophos Firewall product (CVE-2022-1040), weaponize the "Follina" (CVE-2022-30190) vulnerability shortly after discovery and publication, and employ a newly observed custom backdoor we track as LOWZERO in campaigns targeting Tibetan entities."

It is evident that the targeted threat landscape against the Tibetan community is evolving at a rapid pace. Our future requires secure digital infrastructures and serious consideration of the digital security awareness within the Tibetan community. We require collaborative effort of individuals and organizations within the community

9 Androids And iPhones Hacked With Just One WhatsApp Click — And Tibetans Are Under Assault
10 Chinese State-Sponsored Group TA413 Adopts New Capabilities in Pursuit of Tibetan Targets

to overcome a series of cyber attacks of the future, which will be essentially a mixture of advanced social engineering tactics and highly sophisticated types of malware. Zero day attacks against the Tibetan diaspora community is an urgent reminder that we should always stay informed on the latest trends and developments in the online world to protect our digital assets and ensure the security of our devices, accounts and our collective Tibet movement as a whole.

WHO IS BEHIND THE ATTACKS?

A commonly cited challenge of analyzing cyber attacks is the "attribution problem" which refers to the complexity involved in determining with definite certainty who is responsible for cyber attacks and their motives behind it.

Unpacking the attribution problem requires thinking about it across two types: technical attribution and political attribution. Technical attribution refers to how researchers group threat activity into clusters organized around common tactics, techniques, and procedures used by threat actors. For example, malware incidents may share the same server infrastructure or malware tools that suggest the same group is behind the activity or there is some level of resource sharing between connected groups. This type of technical attribution is routine in threat intelligence reports and groups are often identified and tracked based on specific technical characteristics.

A more challenging analytical problem is connecting threat activity to a government sponsor. This is the challenge of political attribution. It is rare for threat intelligence reports to make claims about government sponsorship in part due to difficulties in connecting technical information to government clients and potentially also from liabilities for private companies to make such claims[11]. Notable exceptions include the Mandiant APT 1 report, which describes a cyber espionage campaign against a wide range of targets that operated for years and alleges it is tied to a unit of the People's Liberation Army (PLA). The report showed that the attackers periodically accessed the victim's network to steal sensitive information and intellectual property for a long time, typically maintaining access to victim networks for an average of 356 days. Along with the major U.S. energy companies Threat actors were also found to be able to compromise the email accounts of journalists to steal sensitive information. In a follow up response[12] from the U.S Department Of Justice, five key Chinese

11 Mandiant report on APT1 & China's cyber espionage units
12 U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage

nationals associated with the APT1 were indicted[13] by a grand jury in the Western District of Pennsylvania (WDPA). The 5 members identified were Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui, who are officers in Unit 61398 of the Third Department of the Chinese People's Liberation Army. A report[14] by the Citizen Lab, in April 2010 revealed that APT1 also targeted malware attacks against a Tibetan human rights organization, which shows the group not only targets commercial and industrial sectors but also civil society organizations as well.

Although there is a difficulty of comprehensively identifying the culprit behind targeted attacks against the Tibetan community, there is ample circumstantial evidence that the attacks are orchestrated by the CCP. The first perspective is to consider which nation could be responsible for these targeted attacks against the Tibetan community in exile other than China. Evidence suggests that many documents were exfiltrated/stolen from various offices of Tibetan organizations, many websites disrupted or infected in the past and prominent public figures of the community also targeted with one-click-mobile exploits. The most concerning question is who could have put this much effort when there is nothing much to gain financially from our exile community which is mostly charity and support based. The only inference we can deduce from these attacks sheds light on the intent by the threat actor(s) to disrupt, censor and collect intelligence from our community. In this scenario of political cyber espionage, the most likely culprit is the CCP.

DEFENDING THE COMMUNITY FROM INFORMATION SECURITY THREATS

Cyber threats have been present in the Tibetan community since 2002 and became increasingly pervasive following the protests surrounding the August 2008 Beijing Olympics. 2008 was the year of uprising inside Tibet and also Tibet protests around the world took place in a period of intense and increased resistance activities both on and offline. In the aftermath of 2008, Tibet was under a military lockdown and information blackout. Tibetans in Tibet embraced strategic tactics of self-reliance and noncooperation on a scale never seen before and a new chapter of Tibetan resistance was born.

13 5 Chinese PLA officials accused of cyber espionage on US companies
14 APT1's GLASSES – Watching a Human Rights Organization

Tibet Action Institute was formed in 2009 to support this changing resistance landscape by providing intensive training on lessons of strategic nonviolent action drawn from other successful human rights and democracy movements around the globe. At the same time, Tibet Action Institute became the first Tibet-focused civil society organization to launch education and training programs aimed at helping Tibetans inside and outside Tibet capitalize on new information and communication technologies and defend against relentless cyber attacks and surveillance from China. Tibet Action Institute were pioneers in initiating public awareness events and campaigns on the dos and don'ts in the online world to defend from malicious cyber attacks and sought guidance from, and collaborated with, groundbreaking research groups such as Toronto's Citizen Lab.

When persistent malicious attachment based emails started to emerge in the diaspora community in 2012, Tibet Action Institute launched campaigns such as "Detach from Attachments" and "Think Before you Click" to prevent individuals and organizations from opening or sharing unknown or suspicious attachments and links which might compromise their personal or official systems. In addition to running public awareness campaigns, Tibet Action also initiated a "Digital Security Ambassador" fellowship program aimed at helping key Tibetan NGOs in Dharamsala mitigate digital security attacks. A Tibet Action team member was assigned to support these NGOs navigate technical and digital security difficulties and defend against online threats. Following the success of the fellowship program and in an effort to build community-wide resistance and digital security resilience, Tibet Action Institute established TibCERT - Tibetan Computer Emergency Readiness Team in 2018. TibCERT, based in Dharamsala, India, currently works with over 50 Tibetan stakeholder groups and provides incident response support, digital security policy development and implementation and digital security training. Through TibCERT, three community centers have been established in Dharamsala, Mundgod and Bylakuppe and with over 20 Tibetan volunteers across these centers who support their own network with digital security needs.

This has resulted in a stronger and more digitally secure Tibetan community, capable of proactively addressing online threats and minimizing the risks of cyberattacks. By fostering awareness, building capacity, and creating a network of trained volunteers and organizations, Tibet Action Institute has empowered the Tibetan diaspora to better protect their information and systems. TibCERT's initiatives have not only enhanced the digital security infrastructure but also strengthened collaboration among Tibetan stakeholders, ensuring a united and resilient front against persistent cyber threats. These efforts continue to safeguard both individuals and organizations,

enabling them to focus on their advocacy and cultural preservation without fear of digital compromise.

CONCLUSION

Based on our analysis of public reports and experiences supporting the community, TibCERT has identified a number of areas for increasing online defense against information threats. These include development and implementation of digital security policies, bringing greater awareness of cyber threats and its potential remedies within the community through collaborative training, workshops and other awareness events.

Our recommendations to Tibetans in the diaspora are:

- Recognize that understanding and changing behaviors is as valuable as investing in security infrastructure and tools;
- Recognize the importance of institutionalizing digital security policy to build a safer and more secure framework for day to day online practices;
- Recognize the importance of having a well-informed and knowledgeable dedicated webmaster (or systems administrator) to maintain the security and privacy of its IT infrastructures through identification, prevention and mitigation of such cyber threats in the future;
- Host website security training for current and future upcoming webmasters of the Tibetan diaspora community.

In conclusion, as the Tibetan community builds resiliency and growing awareness around targeted attacks, the threat actors are also raising their cyber espionage efforts. This raises the cost for the threat actors and as it is well known in strategic non-violence techniques that raising the cost for China is half the battle. This research allows Tibetans, and other communities under attack, to understand the threats and also through models like TibCERT, demonstrate how a diaspora community can build resilience, effectively protect itself and raise the cost of continued attacks.

APPENDIX

1. List of web-based cyber attacks against the Tibetan diaspora community

S.No	Year	Website	Owner	Threat Description
1	2008	tibet[.]com	Tibetan Government In Exile	Embedded with a malicious JavaScript file named tibet.js containing iFrame tags pointing to malware files. This Graphical Device Interface (GDI) exploit gives the remote user complete control over vulnerable systems.
2	2012	gyalwarinpoche[.]com	OHHDL	The vulnerable devices connecting to the site were compromised through a backdoor named OSX/Bckdr-RNW allowing attackers to steal data from the system and capture the victim's keystrokes.Two critical vulnerabilities exploited in is attack are CVE-2012-4681 and CVE-2012-0507
3	2013	tibhomes[.]org	Tibetan Refuge School, Mussoorie	Injecting the site with Lady Boyle swf exploit by exploiting the CVE-2013-0634
4	2013	tibetangeeks[.]com	Collective site of Tibetan Tech Enthusiasts	Injecting the site with Lady Boyle swf exploit by exploiting the CVE-2013-0634
5	2013	vot[.]org	Voice Of Tibet	Injecting the site with Lady Boyle swf exploit by exploiting the CVE-2013-0634
6	2013	tibet[.]net	Central Tibetan Administration	The Chinese version of the site is infected with a Java exploit named "YPVo.jar" which drops and executes malicious executables to its visitors. The attack was found to be using an older CVE-2012-4681 vulnerability used a year earlier in August, 2012.
7	2019	Various websites in the Tibetan diaspora	Websites associated with personalities, public bodies, charities and organizations of the targeted group	Malicious two stage Java Script embedded in the site triggered a drive by download of a fake Adobe Flash update. The visitor is then expected to fall into the update trap, and download a malicious installer package that will set up a backdoor.

DISCLAIMER : This report is an outcome of public reports and other open source data available on targeted threats against the Tibetan diaspora community, published by various cyber security research firms and institutions. Neither internal local reports of concerned stakeholders are included in this report nor of any private based companies and institutions. This report is also a result of the lessons learned through our hands-on experience as TibCERT in responding to digital security incidents to our various stakeholders for the past many years since its inception. However this report doesn't encompass all the data associated with targeted threats against the Tibetan community to date and only includes public reports

and incidents prior to 2022. Research report updates from 2022 till now are not mentioned in this report.

ACKNOWLEDGEMENTS : We are grateful to Masashi Nishihata for his tireless guidance on this research report. Furthermore thanks to our Tibet Action Team members including Kate Woznow, Kathy Ní Keefe, Lobsang Gyatso Sither and Tenzin Choedon for their collective effort and engagement in the development of this report.

ADDENDUM

The above technical analysis report and its accompanying narrative report highlight the impact and harm caused by the relentless attacks against the Tibetan community prior to 2022. The Tibetan community continues to face digital attacks and following are some significant attacks that have taken place since 2022.

- A report[15] published by Recorded Future in Sept 2022, the infamous CCP state sponsored group TA413 exploited a zero day vulnerability targeting the Sophos Firewall product (CVE-2022-1040) and leveraged the "Follina" (CVE-2022-30190) vulnerability to deploy newly observed custom backdoors targeting the Tibetan community. In addition to threat actors reusing the same phishing email address tseringkanyaq@yahoo[.]com and mediabureauin@gmail[.]com, a new sender domain name tibet[.]bet was used in their infrastructure to deploy malicious RTF files intended to exploit vulnerabilities in Microsoft Equation Editor (CVE-2017-11882, CVE-2018-0798, CVE-2018-0802). The domain tibet[.]bet was also used in spear phishing attempts targeting an entity associated with the Tibetan government-in-exile. In this activity, the attackers spoofed the Central Tibetan Administration and used a theme of a photography grant intended to support female photographers within the Tibetan community.
- A report[16] published by Volexity in Sept 2023, threat actor group EvilBamboo (formerly named Evil Eye) were found to create fake Tibetan websites such as tibetone[.]org and ignitetibet[.]net along with social media profiles to deploy browser based exploits. Telegram groups were used to push malicious Android applications named AlpineQuest and similar iOS applications named TibetOne available in the Apple App Store, which has since then been removed. Researchers at the Volexity attribute CCP state sponsored threat campaign EvilBamboo (formerly named Evil Eye) behind these attacks targeting Tibetan, Uyghur, and Taiwanese individuals and organizations.
- A report[17] published by ESET in March 2024, the website of Kagyu Monlam was compromised in Jan 2024 through a watering hole attack in which the site displayed a fake error page to entice the user to download a "fix" named certificate (with a .exe extension for Windows or .pkg if macOS). This file is a malicious downloader that deploys the next stage in the compromise chain. In the investigation, one supply chain compromise was detected on one another site which hosts Tibetan language translation software for general users. The attackers placed several trojanized applications there that deploy a malicious downloader for Windows or macOS. The applications finally installs either Nightdoor malware or MgBot malware framework which was later found to be hosted at http://tibetpost[.]net/ OR 188.208.141.204:80 OR 188.208.141.204:5040. This attack attempted to leverage the surge of website visitors during the Monlam Festival religious gathering held annually in January in the city of Bodhgaya, India targeted users in India, Taiwan, Hong Kong, Australia, and the United States. A final malicious nightdoor payload located at [https://update[.]devicebug[.]com]
- A report[18] published by Recorded Future in November 2024, two Tibetan websites namely Tibet Post (tibetpost[.]net) and Gyudmed Tantric University (gyudmedtantricuniversity[.]org) were compromised where attackers exploited vulnerabilities in the Joomla content management system (CMS) used by these sites to implant malicious JavaScript. The site visitors were tricked into downloading a disguised security certificate to deliver the Cobalt Strike malware often used by threat actors for remote access and post-exploitation. The researchers had attributed Chinese state-sponsored threat group TAG-112 and TAG-102 (Evasive Panda) behind these recent targeted web attacks.
- At the same time, our team provided multiple incident responses to other digital attacks ranging from the waterhole attacks to phishing attacks. These attacks were not reported publicly and were addressed by our digital security team when notified of these attacks through our partners and TibCERT member stakeholders.

15 Chinese State-Sponsored Group TA413 Adopts New Capabilities in Pursuit of Tibetan Targets
16 EvilBamboo Targets Mobile Devices in Multi-year Campaign
17 Evasive Panda leverages Monlam Festival to target Tibetans
18 China-Nexus TAG-112 Compromises Tibetan Websites to Distribute Cobalt Strike