Shifting Tactics: Tracking changes in years-long espionage campaign against Tibetans - The Citizen Lab

March 10, 2016

By Jakub Dalek, Masashi Crete-Nishihata, and John Scott-Railton

Summary

This report describes the latest iteration in a long-running espionage campaign against the Tibetan community. We detail how the attackers continuously adapt their campaigns to their targets, shifting tactics from document-based malware to conventional phishing that draws on "inside" knowledge of community activities. This adaptation appears to track changes in security behaviors within the Tibetan community, which has been promoting a move from sharing attachments via e-mail to using cloud-based file sharing alternatives such as Google Drive.

We connect the attack group's infrastructure and techniques to a group previously identified by Palo Alto Networks, which they named Scarlet Mimic. We provide further context on Scarlet Mimic's targeting and tactics, and the intended victims of their attack campaigns. In addition, while Scarlet Mimic may be conducting malware attacks using other infrastructure, we analyze how the attackers re-purposed a cluster of their malware Command and Control (C2) infrastructure to mount the recent phishing campaign.

This move is only the latest development in the ongoing cat and mouse game between attack groups like Scarlet Mimic and the Tibetan community. The speed and ease with which attackers continue to adapt highlights the challenges faced by Tibetans who are trying to remain safe online.

Background

The Tibetan community has been the target of malware-enabled espionage campaigns for over a decade. The attackers responsible for these campaigns are relentless in their attempts to compromise networks and harvest sensitive information. These attacks often demonstrate high levels of sophistication in the social engineering used to entice targets to open malicious attachments or links, but are typically not very technically advanced. A common technique is the use of document-based malware. In a recent four-year study on targeted malware attacks against civil society, which included six Tibetan groups, we found that document-based malware was the most common attack vector, accounting in some cases for up to 95 percent of all attacks against specific Tibetan groups.

The Tibetan community has recognized these patterns and made efforts to change user behaviors to mitigate the attacks. For example, groups have started a digital security training campaign called "Detach from Attachments", which urges users to avoid sending or opening email attachments, and to use cloud-based storage (e.g., Google Drive) to send files instead. However, as the community

changes behaviors, so do the attackers.

Recently, Palo Alto Networks reported on a years-long espionage campaign they call "Scarlet Mimic" that targeted Tibetan and Uyghur groups (as well as government agencies in Russia and India). The Scarlet Mimic campaigns are a typical example of the attacks civil society faces. Carefully crafted email lures are sent to targets carrying exploits that leverage well-known vulnerabilities (e.g., CVE-2012-0158&lt, CVE-2010-3333), which we have seen used in campaigns against Tibetan groups frequently in recent years.

In this post, we show that servers used as malware C2 infrastructure by Scarlet Mimic are now hosting phishing pages designed to steal Google credentials from Tibetan activists and journalists. This shift in tactics from malware to phishing campaigns suggests that the attackers are adapting to behavioral changes in the Tibetan community. In the following sections, we provide an overview of malware campaigns connected to Scarlet Mimic we observed targeting Tibetan groups from 2013-2014, and analyze how the same infrastructure is now being used to host a wave of phishing attacks. We conclude with discussion of what may have motivated this change in tactics, and provide recommendations for targeted users.

Part 1: Scarlet Mimic Campaigns against Tibetans

According to Palo Alto Networks, Scarlet Mimic has been active for at least four years. The attack group primarily uses well-known vulnerabilities and the "FakeM" malware family first reported by Trend Micro in 2013, which attempts to disguise its malicious traffic as commonly used protocols.

A cluster of Scarlet Mimic attacks used the FakeM Custom SSL variant and were deployed on C2 infrastructure that relied on free domains provided by Securepoint, a German dynamic DNS service. Dynamic DNS services typically allow anyone to make free subdomains from a main domain. In the case of Securepoint, this service allows anyone to make free subdomains from `*.firewall-gateway.com`, `*.my-gateway.org`, `*.myfirewall.org` and others. We speculate that the attackers may have selected this particular service, because the domains have innocuous technical names (e.g, `*.firewall-gateway.com`) that may escape casual scrutiny. These kinds of domains can change ownership over time and may be shared by many unrelated users, which can also make analysis more challenging.

Our analysis of attacks against the Tibetan community reveals a series of campaigns active from 2013 to 2014 using the FakeM Custom SSL variant and dynamic DNS infrastructure that is linked to Scarlet Mimic. These malware samples are described in detail in the Palo Alto Networks Scarlet Mimic report. Through our engagement with the targeted groups, we provide further context that demonstrates the level of social engineering and targeting put into the attacks. Understanding this context provides insights into the attackers' tactics, including their later pivot to phishing campaigns.

Campaign 1

The first attack that we connected to Scarlet Mimic was observed in a July 3, 2013 e-mail. The email was sent to the internal mailing list for a steering committee of a Tibetan NGO, and was highly customized. The message spoofed the e-mail of the NGO's director, and demonstrated familiarity with the internal workings of the organization. Under the pretext of an updated strategic plan, the e-mail encouraged recipients to open the attached document titled "[Organization Name] Updated Strategic Plan.doc"

From: [Redacted]
Date: 03 Jul 2013
Subject: Re: [Steering Committee] conclusions to Strategic Plan Review
To: [Redacted]
Dear Steering Committee Members, Thanks everyone for all of the good suggestions! Here is the Updated Strategic Plan and we're looking forward to more comments please!
[Redacted signature]
The malicious attachment installs the file `pshvb.exe` with the MD5 hash:

`8b83fc5d3a6a80281269f9e337fe3fff`
This hash matches a FakeM Custom SSL variant sample described in the Palo Alto Networks report. The malware connected to a C2 server on the domain: `news[.]firewall-gateway[.]com`. At the time of the attack this domain resolved to the IP address `109[.]169[.]77[.]230`, and was hosted on UK-based virtual server provider iomart

Campaign 2

We observed the attackers again on March 19, 2014 when they targeted a different Tibetan group. The attack masqueraded as a message from a representative of the Office of His Holiness the Dalai Lama (HHDL) in Taiwan and contained an attachment that referenced an upcoming visit of HHDL to Japan.

Similar to the previous attack, the attachment dropped the FakeM Custom SSL variant, and is also referenced in the Palo Alto Networks report. In this case the malware connected to the C2 `detail43[.]myfirewall[.]org`, which at the time of the attack also resolved to the same IP address as the previous campaign, `109[.]169[.]77[.]230`.

Another set of attacks spanned from June to July 2014 targeting the same Tibetan group and a number of Tibetan journalists. The Tibetan group received multiple e-mails purportedly from NGOs working on Tibetan issues, while the journalists were enticed by a promise of survey results on Tibetan political attitudes.

All of these attacks used the same FakeM Custom SSL variant and connected to the C2 `sys[.]firewall-gateway[.]net`, which resolved to `95[.]154[.]195[.]159` at the time of the attack and was also hosted on UK server provider iomart. See Figure 1 for an overview of the campaign.

Figure 1: Overview of Campaign 2, showing how the same malicious files are spread using different pretexts.

Part 2: Old Infrastructure, New Tricks

Throughout November 2015 we observed Scarlet Mimic's C2 infrastructure being repurposed to host phishing attacks against the Tibetan community. The phishing campaign we identified consisted of targeted emails with email senders and messages that are relevant to the Tibetan community. The emails appeared to share links to documents or videos on Google Drive or video sharing websites.

The Phishing Campaign

Using the example of an e-mail sent to Tibetan journalists, we can demonstrate how a typical phishing attack in the campaign works. The e-mail masquerades as sent by a Tibetan activist, describes a video on China and Tibet, and shares a link to what appears to be a video sharing site.

From: Dorjee Tenzin <tenzinsft@gmail.com>
Date: 22 Nov 2015
Subject: How CHINA takes care of Tibet and Tibetans – video
To: [Redacted]
This video – How CHINA takes care of Tibet and Tibetans – is short and easy to understand. Must watch.
http://www.downvids.net/how-china-takes-care-of-tibet-and-tibetans-595657.html
In fact, the link directs the user to a phishing page:

`http://accountgoogle[.]firewall-gateway[.]com/serviclogin`

The site displays a lookalike to the Google Gmail login page (see Figure 2).

Figure 2: Comparison of Google login phishing page (left) and authentic Google login as of March 2016 (right).

Interestingly, the login page used by the attackers is slightly outdated. Their version includes both username and password prompts on the same page. Google has been using a two-prompt process for authentication since May 2015

If a victim enters their credentials, the data is sent to the attackers via an HTTP POST request that is formatted as: `http://accountgoogle.firewall-gateway.com/serviclogin/ojkiojr09[.]asp`.
An example of the data that is sent back to attackers is provided in Figure 3.

User-Agent:	Mozilla/5.0 (Windows NT 5.1; rv:21.0) Gecko/20100101 Firefox/21.0
Referer:	http://accountgoogle.firewall-gateway.net/serviclogin/
Host:	accountgoogle.firewall-gateway.net
Connection:	keep-alive
Accept-Language:	en-US,en;q=0.5
Accept-Encoding:	gzip, deflate
Accept:	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Sent Form Data

signIn:	Sign in
service:	wise
rmShown:	1
pstMsg:	1
PersistentCookie:	yes
Passwd:	a
hl:	en
GALX:	s33VkPkelbI
Email:	a
dnConn:	
continue:	http://drive.google.com/?utm_source=zh-CN&utm_medium=button&utm_campaign=web&utm_content=gotodrive&usp=gtd&ltmpl=drive
checkedDomains:	youtube
checkConnection:	youtube:562:1
bgresponse:	!tLdCkkNEkVqoY45ETPRKgB1yREAKAHI0aGNn3enP7YvPZ_INyhLhwQGvzKbybpxXKAPHzonBjXiM6iw9VwByRSqmm-BaISRfMCy55-i9SQ0xHV2jJeLchPTadfcBRbFGNSTTWhVqbYnCznml_j2iHM2oN3kYaPJRUX2rPKaBfM7ryum282PjS44qAAi2ZIHRQcdwoQ
_utf8:	☃

Figure 3: A sample of the data sent to the attackers. The Email and Password fields are the most relevant.

Decoy Content

Once a user enters their credentials they are redirected to decoy content. In the example attack against Tibetan journalists, if the victim entered their credentials they were re-directed to the video "How CHINA takes care of Tibet and Tibetans" on the video sharing site referenced in the email (see Figure 4).

Figure 4: Screenshot of destination content.

The destination content that the user is sent to is determined by a string in the subdirectory of the URL that has various misspellings of "`servicelogin`". In the emails we collected, we found three subdirectory variations:

`http://filegoogle[.]firewall-gateway[.]com/`**`servicelogin`**
`http://accountgoogle[.]firewall-gateway[.]com/`**`serviclogin`**
`http://accountgoogle[.]firewall-gateway[.]com/`**`servicclogin`**
We speculate that the last part of the URL, "`ojkiojr09`" in our example URL (`http://accountgoogle.firewall-gateway.com/serviclogin/`**`ojkiojr09`**`[.]asp`) may be a campaign code, or a way for the attackers to differentiate on their end who is accessing the phished page, and the destination content to which they should be forwarded. We see a similar string in another of the emails that may be used for this purpose: `http://filegoogle[.]firewall-gateway[.]com/servicelogin/sfwef[.]asp`

Phishing Campaign Timeline

We have observed the campaign active between at least November 9, 2015 to December 18, 2015. During this period we collected three phishing emails sent to Tibetan journalists and NGOs. Monitoring the URLs that link to the phishing page reveals that the destination content to which the user would be forwarded was changed frequently. These changes suggest that the campaign was

active beyond the three emails we collected and the attackers were sending out additional emails with messages linked to the new destination content.

Figure 5 provides a timeline for the campaign and shows when emails were received, the original destination content provided, and changes to the destination content over time. On December 18 the servers were up, but no content was being served in reply to logins.

Figure 5: Timeline of phishing campaign (see Appendix A for full details).

While we only collected three emails during the span of the campaign, changes in the destination content suggest the timing and theme of further phishing attacks. On November 25, 2015 the destination content on URLs 1 and 2 were both changed to climate change-related content.

The content redirected from URL 1 was changed to a public Google Drive folder that contained campaign materials on climate change from a Tibetan NGO. The content redirected from URL 2 was changed to a website used to organize the Global Climate March (`globalclimatemarch.org`), a demonstration to raise climate change awareness.

The climate change theme is significant. During this period Tibetan organizations were taking part in advocacy to raise awareness on climate change in Tibetan areas in anticipation of the United Nations Conference on Climate Change held in Paris, France from November 30 to December 12, 2015.

See Appendix A for details on each attack and destination content change.

Overlap with Scarlet Mimic

Similar to the previous FakeM Custom SSL campaigns, the phishing pages used domains provided by Securepoint's dynamic DNS service:

`filegoogle[.]firewall-gateway[.]com`
`accountgoogle[.]firewall-gateway[.]com`
`detail43[.]myfirewall[.]org`
Similar to the previous malware campaigns, all three of these domains are also hosted on iomart.

We observed the first phishing campaign using this infrastructure in early November 2015. During this time, two of the domains (`filegoogle[.]firewall-gateway[.]com`, `accountgoogle[.]firewall-gateway[.]com`) resolved to the IP address `95[.]154[.]195[.]171`.

We further investigated this IP address through passive DNS data sources in PassiveTotal and found additional domains that match the "`firewall-gateway`" naming scheme observed in the Scarlet Mimic malware campaigns:

`accountsgoogle[.]firewall-gateway[.]com`
`accounts-google[.]firewall-gateway[.]com`
`accountsgoogles[.]firewall-gateway[.]com`

`googlefile[.]firewall-gateway[.]net`
`firewallupdate[.]firewall-gateway[.]com`
`firewallupdate[.]firewall-gateway[.]net`
`drivgoogle[.]firewall-gateway[.]com`

Table 1 shows connections between domains identified by Palo Alto Networks, domains we see used as C2 servers in the previous malware campaigns, and relations to servers hosting the recent phishing campaigns. The overlap in domains and passive DNS records shows the infrastructure relationships between the previous Scarlet Mimic campaigns and recent phishing campaigns.

ASN Name	IP Address	Domain	Citlab Seen	FakeM Custom
HOL-GR hellas online Electronic Communications S.A.,GR	5.54.19.17	drivgoogle.firewall-gateway.com	X	
		admin.spdns.org		X
		firefox.spdns.de		X
		intersecurity.firewall-gateway.com		X
	78.129.252.159	kaspersky.firewall-gateway.net		X
		kissecurity.firewall-gateway.net		X
		opero.spdns.org		X
	87.117.229.109	**detail43.myfirewall.org**	X	X
IOMART-AS Iomart,GB		accountgoogle.firewall-gateway.com	X	
		accountsgoogle.firewall-gateway.com	X	
		accountsgoogles.firewall-gateway.net	X	
		filegoogle.firewall-gateway.com	X	
	95.154.195.171	firewallupdate.firewall-gateway.com	X	

		firewallupdate.firewall-gateway.net	X	X
		googlefile.firewall-gateway.net	X	
		news.firewall-gateway.com	X	X
		sys.firewall-gateway.net	X	X
	109.169.40.172	economy.spdns.de		X
LGI-UPC Liberty Global Operations B.V.,AT	46.127.56.109	mail.firewall-gateway.com		X
NEWMEDIAEXPRESS-AS-AP NewMedia Express Pte Ltd. Singapore Web Hosting Service Provider,SG	192.253.251.118	aaa123.spdns.de		X

Table 1: Comparison of domains and hosting seen by Citizen Lab (labelled “Citizen Lab Seen”) and the FakeM Custom SSL cluster described in the Scarlet Mimic report (labelled “FakeM Custom”).

Evidence of Other Campaigns

We leveraged patterns in the configuration of the phishing servers to identity additional servers. The IP address `95[.]154[.]195[.]171` that we saw previously was using Microsoft IIS web server version 6 and was configured to forbid access to the top level of the URL path. Using the search engine Shodan we scanned all servers on iomart that ran IIS 6 and forbid access to the root url path with the query:

```
port:80 IIS/6.0 forbidden title:Error "Content-Length: 218" country:"GB" org:iomart
```

For all the matched servers we sent a query to the URL path (`/servicelogin/ojkiojr09.asp`), which is used to redirect victims to destination content in the phish attacks. The purpose of this query was to to determine if any other servers would forward us to content in the same manner we had observed in the attacks.

We found one other IP address (`87[.]117[.]229[.]109`) on iomart that responded to this query. We observed this server responding with a redirect to an article by Radio Free Asia regarding the arrest of the aunt of Tenzin Delek Rinpoche, a Tibetan monk who recently died while in a Chinese prison.

We saw this content active from November 30, 2015 to December 3, 2015, when the forward link

stopped working, which may mean that the campaign completed at this time.

We used PassiveTotal to identify which domains pointed to both IP addresses from March 2015 to December 2015 and saw an overlap across three domains:

`sys[.]firewall-gateway[.]net`
`news[.]firewall-gateway[.]com`
`firewallupdate[.]firewall-gateway[.]net`
The domain: `firewallupdate[.]firewall-gateway[.]net` was referenced in the Palo Alto Network report and pointed to both the IPs we identified at different times (see Figure 6).

Figure 6: Domain overlap between two iomart IPs in the phishing infrastructure.

Additionally this new IP had two additional domains that were also using the Securepoint dynamic DNS service: `updata[.]firewall-gateway[.]com` and accounts-google[.]firewall-gateway[.]com. We saw one of the domains: `detail43[.]myfirewall[.]org` used as a C2 server for an attack in the previously described Scarlet Mimic campaign from 2014.

Why the Shift to Phishing?

When Scarlet Mimic shifted tactics, they failed to properly compartmentalize their phishing and malware operations, relying on known C2 infrastructure for the new phishing campaigns. Although they tried different attack vectors they still fell back on old habits and resources that could be leveraged by analysts. Monitoring the infrastructure enabled us to track the campaigns over time and demonstrates the importance of infrastructure analysis for security researchers.

The shift to phishing campaigns is significant, as Palo Alto Networks only observed document-based malware attacks.[1] Importantly, Scarlet Mimic may be continuing to conduct as-yet unreported malware campaigns on other infrastructure. There are a number of potential explanations for this change.

The phishing campaigns targeted multiple organizations and individuals in the Tibetan community. Many of these groups act as distributed networks, with staff members and collaborators around the world. The attackers are, therefore, not necessarily targeting compromise of office networks, but rather social networks. Credential phishing is a potentially more efficient means of gaining access to these networks than document-based malware.

In addition, the promotion of behavioral changes in the Tibetan community and the use of document-sharing platforms such as Google Docs over email attachments may have put pressure on attackers' tactics and led them to experiment with simpler, but potentially effective vectors, such as phishing. In other attacks against the Tibetan community over the past year we have also seen malware sent via Google Drive links in targeted emails. The Scarlet Mimic phishing campaigns add further evidence that attackers are attempting to leverage the wide use and trust of Google applications in the Tibetan community.

It is also possible that the rising detections by antivirus products of Scarlet Mimic's preferred malware toolkit play a role. Out of the 74 FakeM sample hashes provided in the Palo Alto Networks Scarlet Mimic report, 61 are available on VirusTotal. When the samples were first submitted to VirusTotal some had zero detections and an overall average detection rate of 38 percent. Following the publication of the Palo Alto Networks report the average detection increased to 54 percent. The current average detection rate is 71 percent, the highest is 80 percent (46 / 57 antivirus scanners), and the lowest is 51 percent (23 / 45 antivirus scanners). These current detection rates may make the malware that the attackers used in past attacks less reliable for successful infection. While the attackers could be pivoting to new, less detectable malware, simple phishing attacks may also involve less effort and achieve higher success against journalists and NGO targets.

Finally, we cannot rule out that converting burned or low-utility command and control servers to phishing might also be intentional down-cycling of infrastructure, before it is discarded. Phishing, in other words, may be the last stop before domains and servers that are losing value are finally given up.

Conclusion

The Tibetan community has been targeted by sophisticated, persistent attackers for over a decade. Scarlet Mimic is just one of these attack groups, and over the years they have demonstrated deep familiarity and inside knowledge of the Tibetan groups they target. They have also shown themselves to be adaptable and responsive to changes in the security behaviors of their targets.

Their most recent turn to phishing seems to reflect this adaptability (although we leave open the possibility that malware attacks are continuing, using other infrastructure). A number of factors may have played a role in this transition, including an increase in certain security behaviors within the Tibetan community (such as not opening or sending attachments), and increasing rates of detection by antivirus products.

The information targeted by this group is sensitive, and in the hands of a well-resourced adversary, such as the sponsor of Scarlet Mimic, could cause harm to the safety and security of individuals in Tibet. The extracted information could also be used in support of efforts to frustrate and isolate political groups in the Tibetan diaspora.

Phishing relies on tricking users into entering credentials. In this case, there are several telltale signs (such as a slightly outdated Gmail login phishing page) that may suggest to potential victims that something is "not quite right." However, there are also a number of tools and tactics available to users in the Tibetan community and beyond to stay safe online We describe several of these below.

What Can Targeted Users Do?

Tools

- **Use two-factor authentication.** This feature is available on many popular email and social

network services including those from Google, Facebook, Microsoft, Yahoo, and others. Enabling two-factor authentication means you have to enter your password as well as a code provided by a text, app, or security key to access your account. The second factor helps protect you from credential theft.

- **Password Alert** [get it by clicking here] is a Chrome extension developed by Google that notifies you if you enter your Google credentials into any pages other than the real Google login page (https://accounts.google.com).

Behavior

- Always be cautious about emails containing links or attachments and carefully examine the email sender address in suspicious messages.
- If an email contains a link always verify that the domain in the URL matches the link text.
- For further resources on digital security see Tibet Action Institute's Be a Cyber Super Hero project.

Footnotes

1.The one divergence from this pattern that has been previously reported was a 2013 Strategic Web Compromise (SWC) attack against the Tibetan Alliance of Chicago's website documented by WebSense. A SWC is an attack in which attackers compromise normally trusted websites and serve malicious code to specific visitors. In this case, the attackers used the Tibetan website to serve an Internet Explorer vulnerability (CVE-2012-4969) that was patched in 2012. This attack used the domain `mail[.]firewall-gateway[.]com` as a C2, which is from the same dynamic DNS service as the FakeM SSL Custom variant attacks.

Acknowledgements

This research was supported by the John D. and Catherine T. MacArthur Foundation (Professor Ronald J. Deibert, Principal Investigator). Special thanks to PassiveTotal, Ron Deibert, Lobsang Gyatso, Sarah McKune, Adam Senft, and Nart Villeneuve.

Appendix A: Phishing Campaigns in Detail

Phishing Attack 1

The first phishing attack we saw was sent on November 9, 2015 to a group of Tibetan journalists. The message purported to contain a link to a document with information on a controversial Buddhist sect known as Dorje Shugden or Dolgyal, which has been involved in protests against the Dalai Lama.

From: Choephel Tenzin <tenzinch128@gmail.com>
Date: Mon, Nov 9, 2015

Subject: Who is demonstrating against the Dalai Lama
To: [Redacted]
File regarding Dolgyal.
Who is demonstrating against the Dalai Lama.doc
The link “Who is demonstrating against the Dalai Lama.doc” actually goes to `http://accountgoogle[.]firewall-gateway[.]com/servicclogin`. When we first checked this link on November 13, the page was down and we therefore do not know what the original destination content was for this attack.

Destination Content Switch

On November 25 the link was active and the destination content was a public Google Drive folder that contained campaign materials on climate change from a Tibetan NGO. The climate change theme is significant, as during this period Tibetan organizations were taking part in advocacy to raise awareness on climate change in Tibetan areas in anticipation of the United Nations Conference on Climate Change held in Paris, France from November 30 to December 12, 2015.

Phishing Attack 2

The second phishing attack was sent to Tibetan journalists on November 22, 2015.

In this case the email was made to appear to come from a Tibetan activist, describes a video on China and Tibet, and shares a link to what appears to be a video sharing site, but is actually `http://accountgoogle[.]firewall-gateway[.]com/serviclogin`.

From: Dorjee Tenzin <tenzinsft@gmail.com>
Date: 22 Nov 2015
Subject: How CHINA takes care of Tibet and Tibetans – video
To: [Redacted]
This video – How CHINA takes care of Tibet and Tibetans – is short and easy to understand. Must watch.
http://www.downvids.net/how-china-takes-care-of-tibet-and-tibetans-595657.html
On November 22, 2015, if users entered their credentials into the Google login phishing page they would be redirected to the video described in the email.

Destination Content Switch

On November 25, 2015, the destination content was changed to a website used to organize the Global Climate March (`globalclimatemarch.org`), a demonstration to raise climate change awareness around the United Nations Conference on Climate Change.

The November 25, 2015 destination content change shares the timing and theme of the change we observed on the previous URL path variation. While we do not have additional phishing emails from

this period, these commonalities suggest the attackers were sending phishing emails with climate change themes around November 25, 2015.

Phishing Attack 3

On November 23, 2015, an email appearing to be from the Press Officer of the Central Tibetan Administration was sent to multiple Tibetan journalists, activists, and NGO staff members.

From: Tsering Wangchuk <euhrdesk.diir@gmail.com>
Date: 23 Nov 2015
Subject: Press Invitation
To: [Redacted]
Press Invitation
The media is cordially invited by the Election Commission of the Central
Tibetan Administration its press conference regarding the upcoming Sikyong
and Tibetan final elections at Lhakpa Tsering hall, DIIR, on November 27, 2015, at 10:00 AM.
Press Invitation.pdfTsering Wangchuk
Press Officer
+91 8679208465
www.tibet.net
Twitter: https://twitter.com/Pressofficerct
Facebook: https://www.facebook.com/lhuabu
DIIR, CENTRAL TIBETAN ADMINISTRATION

The “Press Invitation.pdf” link actually goes to http://`filegoogle[.]firewall-gateway[.]com/servicelogin`. On November 23, when the email was sent, if the user entered their credentials into the phishing page they would be redirected to a Google Doc containing a copy of an op-ed written by the Central Tibetan Administration on climate change. The destination content and the email message do not match in this case, which may be evidence of the attackers neglecting to switch out content from a previous campaign.

Tibet – Climate Action for the Roof of the World

What do heat waves in Europe and erratic weather patterns in the United States have in common with monsoons, floods and droughts in Asia? The answer is Tibet.

Massive heat waves in Europe this past summer have been linked to thinning snow cover on the Tibetan Plateau. And temperature and atmospheric changes on that same plateau influence the timing and duration of the monsoon season in Asia. In North America, climate change on the plateau has been linked to the increase in severe weather. The Tibetan Plateau's climate-influence is local, regional and global.

Tibet is an environmentally strategic area and its importance to the sustainability of the world's ecosystem cannot be overstated.

At an average elevation of 4000 metres above sea level and with an area of 2.5 million square kilometres, Tibet is the world's highest and largest plateau. Its 46,000 glaciers make Tibet home to the third largest concentration of ice after the South and North Poles. Tibet is literally the roof of the world.

As world leaders gather in Paris for the United Nations COP21 meetings on climate change, Tibet needs to be on the agenda.

Tibet is experiencing dramatic effects of climate change.

In the past 50 years, the Tibetan Plateau's temperature has increased by 1.3 degrees Celsius—three times the global average.

Destination Content Switch

On November 26, 2015, the destination content to which the phishing page redirected users was changed to a Google Drive document that provides the program for a visit to Dharamsala, India by Chilean Parliamentarians.

Tentative program of the visiting Chilean Parliamentarians to Dharamshala

29th November to December 04, 2015

29 November, Sunday

13:30hrs	Arrive at Gaggal Airport by spice jet at 1:30pm and receive by Protocol Officer, Department of Information and International Relations, (DIIR)
14:00hrs	Check in at Chonor House
16:00hrs	Visit Tibet Museum and Tsuglakhang (Namgyal Monastery)

30 November, Monday

9:00hrs	Morning shift reserved for the Audience of His Holiness Dalai Lama with the visiting delegates.
14:00hrs	Visit Library of Tibetan Works & Achieves and meet Geshe Lhakdor la, Director to discuss about secular ethics/introduction to Meditation
15:30hrs	Visit to the Tibetan Medical and Astrology Institute (TMAI) and meet Director, Mr. Tsering Tashi Phuri
17:00hrs	Back to Hotel

Appendix B: Indicators of Compromise

Scarlet Mimic Malware Campaign 1

Binaries

MD5: fef27f432e0ae8218143bc410fda340e

Command and Control Servers

`news.firewall-gateway[.]com`

Scarlet Mimic Malware Campaign 2

Attack 1

File attachments

Filename: `20140317144336097.DOC`
MD5: `3b869c8e23d66ad0527882fc79ff7237`

Binaries

Filename: `cghnt.exe`
MD5: `1bf438b5744db73eea58379a3b9f30e5`