UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

*Join the Global Conversation*

**The Citizen Lab**

**Research Brief**
March 2015

# *Tibetan Uprising Day Malware Attacks*

Authors: Katie Kleemola, Masashi Crete-Nishihata and John Scott-Railton

## SUMMARY

- Hundreds of members of the Tibetan community are being targeted by email-based malware attacks that leverage the March 10 Tibetan Uprising anniversary as a theme.
- This report analyzes two March 10 related attacks. One using a new malware family we call "MsAttacker" that we have not observed before, and another using the ShadowNet malware family and command and control infrastructure related to previous campaigns known to have targeted the Tibetan community.
- We include user recommendations for preventing infection and indicators of compromise for researchers to identify MsAttacker.

## BACKGROUND

On March 10 1959, amidst growing unrest, Tibetans took to the streets of the capital Lhasa to protest the Chinese occupation of Tibet. Thousands surrounded the Potala Palace, then the home of His Holiness the Dalai Lama (HHDL), spurred by fears that he was to be arrested by the Chinese authorities. Following this event, escalation of tensions between Chinese and Tibetan forces led to HHDL escaping Tibet and taking up exile in northern India.

The anniversary of the March 10 Tibetan Uprising is a major event in the Tibetan diaspora, commemorated with a day of protest around the world to raise awareness around Tibetan rights issues. It is a period of intensive activism and mobilization for many Tibetan organizations.

In previous research, we described how attackers leverage the heightened activity around the event with social engineering campaigns, seeding targeted malware.  For example, we have found personalized e-mails that use references to the anniversary to trick recipients into opening malicious attachments.

In this report we analyze two separate email-based targeted malware attacks that use the March 10 anniversary as a theme.

## ATTACK 1: MSATTACKER

On March 5 2015, an email with the subject line “10th March 2015 campaign for Tibet” was sent to hundreds of individuals and organizations from the Tibetan community. The email purported to come from a well-known Tibetan NGO and contained information about a series of events planned to commemorate the 56th anniversary of the Tibetan Uprising.

Attached to the email was a malicious Microsoft Word file “10th March.doc” that used the exploit CVE-2012-0158, which is a vulnerability in how Microsoft Word handles RTF documents. This vulnerability has been patched since April 10, 2012 but has remained the most frequently used CVE we have observed in malware attacks against Tibetan groups for the last two years. Its repeated usage suggests that attackers are successfully compromising members of the community, because their systems do not have the latest software updates. The exploit was used to deliver a malware family that does not match any available signatures and has not been observed by us in previous attacks against the Tibetan community.

The malware first connects to a command and control server (C2) 122.10.117.152 located in Guangzhou, China.

The malware then downloads a stage 2 binary: [c2 ip]/download/ms/MiniJs.dll

This file is copied to  c:\windows\system32\teamviewsvc.dll and creates a service to run on startup. It then connects to 23.27.127.200 to receive further requests.

We call this family “MsAttacker” after an event name in the stage 2 binary.

We were also provided with another sample of MsAttacker that was also sent on March 5 in a highly targeted attack against a Tibet-related NGO. The email contained information about a private event the group was planning that was unrelated to March 10 activities. The attachment contained the same payload as the first March 10 related attack.

We found one other example of this malware in the wild. On March 5, an analysis of a file “WTO. non-market status China _1_.doc” was posted to Malwr (a community malware analysis platform). This sample was from the same family and also connected to 122.10.117.152.

## ATTACK 2: SHADOWNET

In another attack on March 5, members of a Tibetan human rights organization received an email appearing to come from the group’s organizational mailing list. The email message contained information from the secretary of the Bureau of His Holiness the Dalai Lama regarding events related to March 10. Attached was a malicious Microsoft Word file that had the same filename as the previous attack (10th March.doc) and also used CVE-2012-0158. However, the malware used in this attack is from the ShadowNet family.

ShadowNet malware leverages Windows Management Instrumentation (WMI), a system tool meant for administrators. Its intended usage as a tool for collecting system information and automation makes it an ideal mechanism for gathering and exfiltrating data. The use of legitimate Windows features can make it more difficult for administrators to identify activity as malicious.

ShadowNet typically uses multi-layered C2 infrastructure that first connects to blog websites and then retrieves C2 information from encoded strings left on the blog. By using blog sites as intermediaries the attackers can maintain control of compromised machines even if a C2 is blocked by a network firewall or otherwise goes down. If a C2 needs to be updated the attackers can simply point the intermediaries to new servers.

The sample used in this attack includes a WMI Script with links to three blogs (hxxp://johnsmith152.typepad.com/blog/rss.xml; hxxp://mynewshemm.wordpress.com/feed/; hxxp://johnsmith5382.thoughts.com/feed). The blogs contain an encoded string that points to the actual C2: hxxp://www.semamail.info/firex/test.php, which has the IP 122.10.117.5 and is on the same Autonomous System (AS 24544) as the C2 for the MsAttacker sample. Apart from this commonality and the timing of the attack we do not observe any other linkages between the MsAttacker and ShadowNet attacks.

The domain (semamail.info) has questionable whois information:

Registrant Name: Kasong Dolma
Registrant Street: New York
Registrant City:New York
Registrant State/Province:guangdong
Registrant Postal Code:10001
Registrant Country:CN
Registrant Phone:+1.9175608889
Registrant Email: mike.fly@email.com

This same registration information has been used for a number of other domains including conamail.info, convmail.info, and fifamp3.info. The domain fifamp3.info resolves to 122.10.117.35. Passive DNS records show that the same IP has pointed to rukiyeangel.dyndns.pro, which is related to C2 infrastructure used in the Lucky Cat and TseringKanyaq campaigns.  ShadowNet was also used in both of these campaigns. The overlap between C2 infrastructure and malware families suggests some level of coordination between this new attack and the previous campaigns.

## CONCLUSION AND RECOMMENDATIONS

These attacks are a reminder that members of the Tibetan community are consistently targeted, and that the threat seems to increase during important Tibetan events.

These kinds of  attacks can be mitigated through greater user awareness and changes in behaviour. Users in targeted communities should always be cautious about unsolicited emails containing links or attachments and should carefully examine the email sender addresses in suspicious messages.

Viewing documents through the Gmail preview feature, or by uploading them to Google Docs to view them can make it possible to look at the content of attachments without risking infection of a machine.  Suspicious files can also be submitted to VirusTotal (but should not be submitted if the files contain personal information) or shared with technical experts within the community.

For further resources on digital security the Citizen Lab recommends Tibet Action Institute's Be a Cyber Super Hero project. We are continuing to closely analyze these attacks and the MsAttacker malware family.

We will post further details as they become available.

## INDICATORS

### *MsAttacker Samples*

**Stage 0**

**MD5**: 8346b50c3954b5c25bf13fcd281eb11a **SHA1:** d9a74528bb56a841cea1fe5fa3e0c777a8e96402 **SHA256:** de7058700f06c5310c26944b28203bc82035f9ff74021649db39a24470517fd1

**Stage 0**

**MD5**: 6fc909a57650daff9a8b9264f38444a7
**SHA1:** 2a2a1fae6be0468d388aa2c721a0edd93fb37649
**SHA256:** a264cec4096a04c47013d41dcddab9f99482f8f83d61e13be4bcf4614f79b7a0

**Stage 1**

**MD5**: 69a0f490de6ae9fdde0ad9cc35305a7d
**SHA1:** e3532fc890f659fb6afb9115b388e0024565888c
**SHA256:** 3de8fb09d79166f10f4a10aef1202c2cb45849943f224dc6c61df8d18435e064

**Stage 2**

**MD5**: 2782c233ddde25040fb1febf9b13611e
**SHA1:** be50ef6c94f3b630886e1b337e89f4ea9d6e7649
**SHA256:** 50aebd2a1e3b8917d6c2b5e88c2e2999b2368fca550c548d0836aa57e35c463f
**C2s**
122.10.117.152
23.27.127.200

### *Ms Attacker Identifiers*

**Stage 1 Strings**

```
http://122.10.117.152/download/ms/CryptBase.32.cab
http://122.10.117.152/download/ms/CryptBase.64.cab
http://122.10.117.152/download/ms/MiniJS.dll
MiniJS.dll
gupdate.exe
rundll32.exe %s install %s
%s;new Downloader('%s', '%s').Fire();
rundll32.exe %s RealService %s
```

**Stage 2 Strings**

```
MiniJS.dll
RealService
%s "rundll32.exe %s RealService %s" /f
reg delete HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "Start Pages" /f
TeamView
3111431114311121270018000127001808012700180
Global\MSAttacker %d
```

***ShadowNet Samples***

**Stage 0**

**MD5:** 72707089512762fce576e29a0472eb16
**SHA1:** 4ab039da14acf7d80fbb11034ef9ccc861c5ed24
**SHA256:** ddfa44ebb181282e815e965a1c531c7e145128aa7306b508a563e10d5f9f03fb

**Stage 1**

**MD5:** d8ae44cd65f97654f066edbcb501d999
**SHA1:** 602a762dca46f7639210e60c59f89a6e7a16391b
**SHA256:** e8f36317e29206d48bd0e6dd6570872122be44f82ca1de01aef373b3cdb2c0e1

**C2s**
hxxp://www.semamail.info/firex/test.php (122.10.117.5)

## ACKNOWLEDGEMENTS

Thanks to Chris Davis, PassiveTotal, and Adam Senft.