UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

The Citizen Lab

Research Brief
July 2012

Recent Observations in Tibet-Related Information Operations: Advanced Social Engineering for the Distribution of LURK Malware

KEY FINDINGS

- Social engineering techniques observed in recent targeted malware attacks against Tibetan organizations appear to repurpose authentic, privately-held, sensitive content of Tibetan groups -- in contrast to typical malware attacks that rely on simpler social engineering methods, such as referencing themes of interest to the organization or copying publicly available legitimate content. The use of this unique content suggests that attackers may have achieved a preliminary level of infiltration into Tibetan organizations, which could allow them to increase the apparent authenticity of subsequent attacks.

- These recent malware attacks have incorporated a "passwording" technique, whereby attached, infected Microsoft Office files are encrypted and can only be opened with a password provided in the email body.

- The payload of each of these targeted malware attacks is the LURK malware, a remote access trojan that is a variant of Gh0stRAT.

- Once active, the malware delivered through each of these targeted attacks connects to the same command-and-control server: dtl.dnsd.me:63 (184.105.64.183), which if inaccessible uses a backup domain, dtl.eatuo.com:63. Both dnsd.me and eatuo.com are dynamic DNS providers, and eatuo.com has the same domain registration information as the well-known Chinese provider 3322.net.

BACKGROUND

This blog post is the third in a series documenting the use of information operations against Tibetans and others who advocate for Tibetan rights and freedoms.

Previous research by the Citizen Lab has described information operations that leveraged the issue of self-immolations amongst Tibetans, as well as a recent European Parliament resolution on the human rights situation in Tibet.

OVERVIEW

In its ongoing study of targeted cyber threats against civil society organizations, Citizen Lab has analyzed 11 malicious emails sent to Tibetan organizations between May and July 2012 that display noteworthy common elements, including malware that connects to the same command-and-control server.

Attackers have targeted at least three separate organizations, sending the malicious emails to seven different email addresses associated with those three organizations.

In each of these emails, the malicious file is password-protected, such that it can only be opened with a password provided in the email text (or in one case, in an image attached to the email), and the payload -- LURK malware -- is the same.

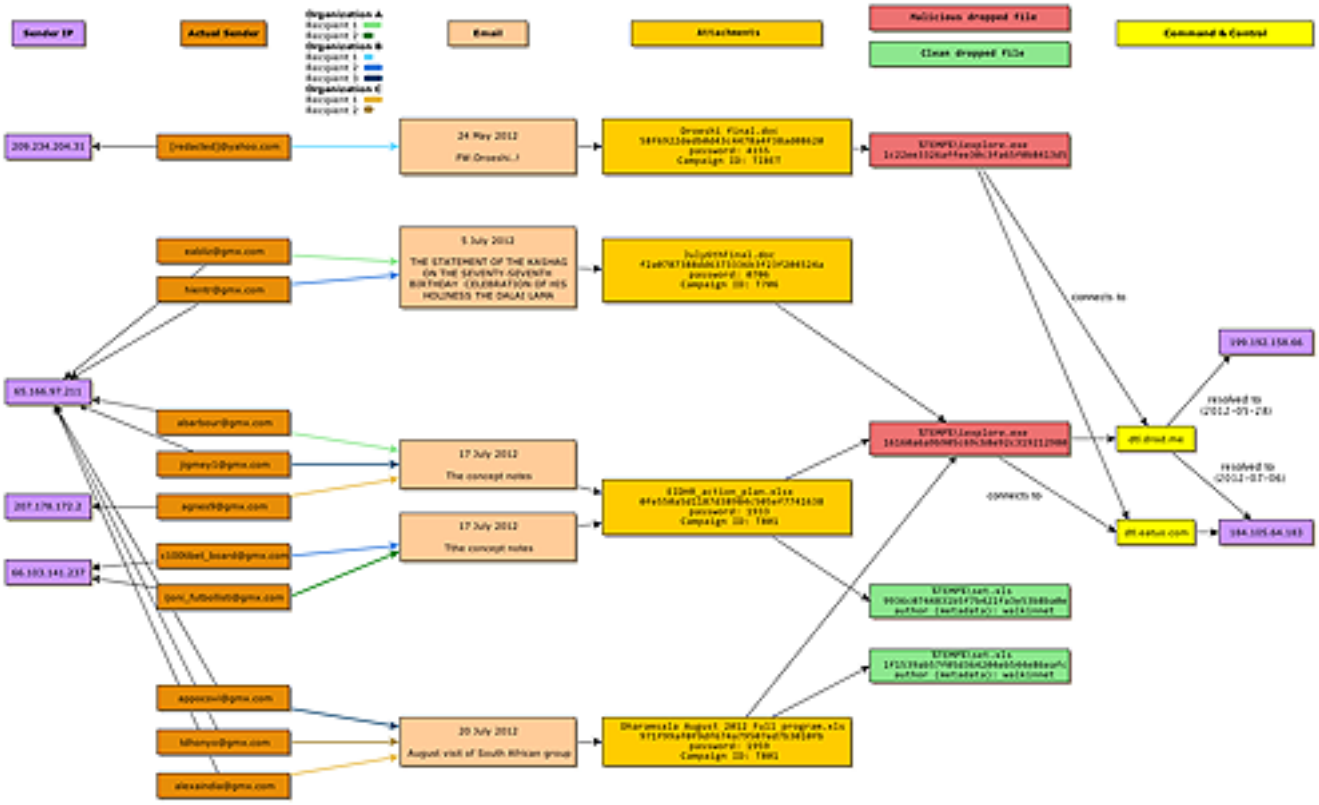
The level of authenticity of the social engineering used in these emails, however, has increased over time, with the most recent emails repurposing sensitive content of Tibetan groups that was most likely privately held and/or inaccessible to the general public.

The use of such content suggests that attackers may have achieved a preliminary level of infiltration into Tibetan organizations, which could allow them to accomplish more advanced and effective social engineering, thereby increasing the risk of compromise.

TARGETED MALWARE ATTACKS

In the 11 emails there are four distinct messages used in the attacks, as outlined and illustrated below. The malicious attachments are all Microsoft Office documents -- two Word documents and two Excel files -- that are encrypted using four-digit numeric passwords, perhaps in an attempt to prevent detection of the malicious file by antivirus software, or to increase the apparent authenticity of the document.

The passwords appear to have been chosen to reflect dates of historical significance with respect to Tibet -- for example, 1959 was the year of the Tibetan uprising against the rule of the Communist Party of China, which is commemorated by the Tibetan community every year on March 10. The malicious payloads all communicate with the same command-and-control (C2) server (discussed further below).



1. "Droeshi"

The first email, which was only sent to one email address of which we are aware, was sent on May 24, 2012 from what appears to be a compromised yahoo.com email account associated with a Tibetan activist, from the IP address 209.234.204.31 (likely a compromised server):

FW:Droeshi..!

Date: 24 May 2012

Subject: FW:Droeshi..!

Dear

Please find attached here three paged agenda for the upcoming meeting in June 2012. Since we will not be sending them by post, you are all requested to print them out and treat them as fair copies. At the same time, please don't fail to acknowledge this mail. Thank you so much.

Pass:4155

warm regards,

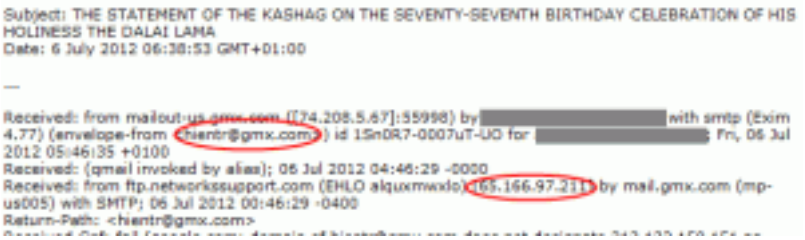
Attachments

- Droeshi final.doc

Note that the salutation does not include the name of the recipient, nor is it signed. The password required to open the attachment is 4155.[1] The attachment is a Word document named Droeshi final.doc -- when opened and supplied with the password, it crashes Word and drops its malicious payload (described in more detail below). No clean file is dropped or shown to the user, and there is no author or summary metadata.

2. "Statement of the Kashag"

The second email was sent on July 5 to at least two different organizations. The body of these emails contains only "PASSWORD: 0706."[2] The subject is "THE STATEMENT OF THE KASHAG ON THE SEVENTY-SEVENTH BIRTHDAY CELEBRATION OF HIS HOLINESS THE DALAI LAMA" and the "From" address spoofs the real address of a Tibetan organization. Although the emails are identical and were sent from the same IP address (65.166.97.211), the actual email addresses used to send each message differ: eabliz@gmx.com and hientr@gmx.com (click image to enlarge).


Subject: THE STATEMENT OF THE KASHAG ON THE SEVENTY-SEVENTH BIRTHDAY CELEBRATION OF HIS HOLINESS THE DALAI LAMA
Date: 6 July 2012 06:38:53 GMT+01:00

—

Received: from mailout-us.gmx.com ([74.208.5.67]:55998) by [redacted] with smtp (Exim 4.77) (envelope-from <hientr@gmx.com>) id 1Sn0R7-0007uT-UO for [redacted]; Fri, 06 Jul 2012 05:46:35 +0100
Received: (qmail invoked by alias); 06 Jul 2012 04:46:29 -0000
Received: from ftp.networkssupport.com (EHLO alquxmwxlo) [65.166.97.211] by mail.gmx.com (mp-us005) with SMTP; 06 Jul 2012 00:46:29 -0400
Return-Path: <hientr@gmx.com>

This email also attached a single Word document, July6thFinal.doc, that exhibits similar behaviour to the Droeshi document but drops a slightly different malicious executable.

3. "The concept notes"

The third email came in two versions on July 17, differing only in an additional blank line in the email body and a typo in the subject line of one version. The social engineering has been significantly stepped up in this attack, though there are still numerous tell-tale signs that it is not legitimate. This email had five attachments: four benign .docx files, as well as a malicious Excel file named EIDHR_action_plan.xlsx.

Tthe concept notes

Date: 17 Jul 2012

Subject: Tthe concept notes

Dear,

PC sent me this e-mail along with all the attachments. I hope these are not the documents containing the sensitive infos.

password 1933

Best regards,
[REDACTED]

Attachments

- CONCEPT_NOTE_1.docx
- CONCEPT_NOTE_2.docx
- Dept_of_Religion_EIDHR.docx
- EIDHR_action_plan.xlsx
- The_concept_note_PC.docx

Again there is no name in the salutation, but the email is signed in this case. The signature and "From" address used spoof a representative of the Office of Tibet.

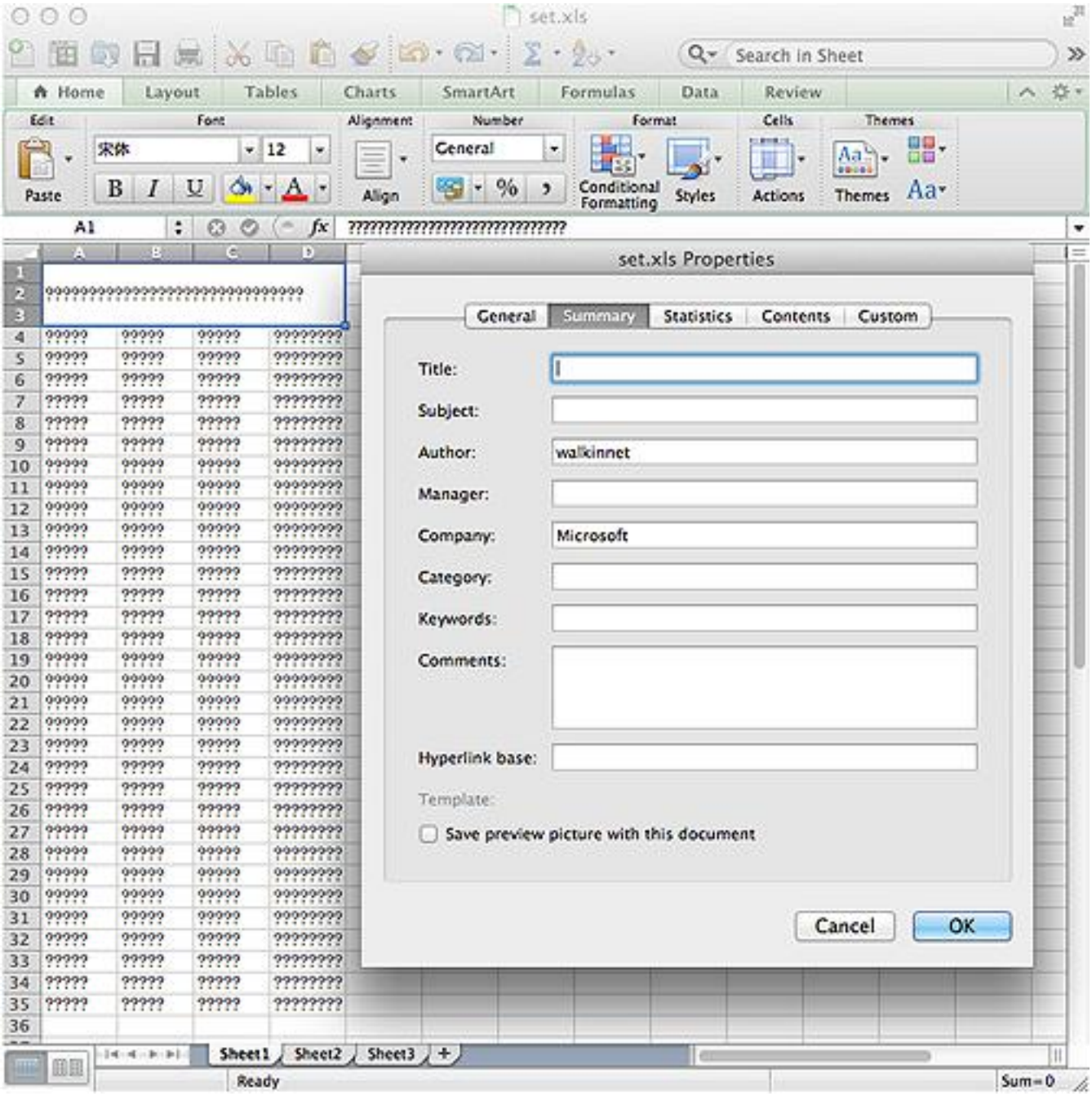
The Word documents attached to this email contain what appears to be an actual application by a Tibetan organization to the European Instrument for Democracy and Human Rights (EIDHR).

The timing of this attack is particularly noteworthy in that a genuine EIDHR call for proposals -- including for "Actions Aimed at Fighting Cyber-Censorship and to Promote Internet Access and Secure Digital Communication" -- was pending at the time, with a July 20 deadline for concept notes.

Such documentation related to grant proposals is typically of a sensitive and internal nature to civil society organizations, and inclusion of such content in a targeted malware attack is concerning, as it suggests access to confidential materials and perhaps even awareness of the parameters of the EIDHR call.

Only the attached malicious Excel file requires the password -- 1933[3] -- to open, whereas the attached Word documents are not password protected. The malicious Excel file is actually an OLE file, not the newer Office Open XML format that the .xlsx extension suggests, and Excel refuses to open it unless the extension is changed to .xls. The dropped malicious executable is identical to the one from the "Statement of the Kashag" email.

This file also drops a clean document, “set.xls,” in the user’s temporary folder and opens it in Excel. The contents of the file were unreadable on all computers we tried it on, displaying only question marks. However, the metadata of the file shows the author as ‘walkinnet’ (click image to enlarge).



We saw five instances of this message, going to three different organizations. The email with the typo in the subject ("*Tthe concept notes*") went to two different organizations, from a different IP (66.103.141.237) than the *“Statement of the Kashag*” email. Different gmx.com addresses were used to send each message: c100tibet_board@gmx.com and ijoni_futbollisti@gmx.com.

The other three instances of this email had the subject "*The concept notes*" and were sent by yet more unique gmx.com addresses: abarbour@gmx.com, jigme1@gmx.com and agnes9@gmx.com. The first two were sent from the same IP as used for the "*Statement of the Kashag*," but the third came from 207.178.172.2.

4. "August visit of South African group"

The most recent email was sent on July 20 to at least two organizations, one of which received it at two different addresses. The email contains text and an Excel attachment that, as with the "*The concept notes*" email, suggest the attacker had access to confidential communications of a Tibetan organization.

The spoofed "From" address, subject ("*August visit of South African group*"), and text of the email all appear to be repurposed from an authentic message sent to a Tibetan organization from a person seeking advice regarding an upcoming trip to Dharamsala, and the content includes in-depth details on trip logistics and planning.

In this case, the password required to open the attached Excel file is not in the body of the email, but added (rather awkwardly) to an attached image of the logo of the organization belonging to the spoofed sender. The password is "1959," the year of the aforementioned Tibetan uprising.

The attached Excel file, Dharamsala August 2012 Full program.xls, is similar to the malicious attachment in "*The concept notes*" email, but it drops a different clean file. In this case the file is readable and contains what is almost certainly an authentic itinerary, which is referenced in the email. The clean file is also called set.xls, defaults to the same Chinese font, and has the same 'walkinnet' author metadata as the clean document in "*The concept notes*."

TECHNICAL ANALYSIS

Delivery Methods

Within the dataset examined by Citizen Lab, two Word documents and two Excel documents were sent embedded with LURK malware, a remote access trojan that is a variant of Gh0stRAT. Note that the XLSX file is actually a standard .XLS file, not the new XML format.

The MD5 hashes of the documents are as follows:

Droeshi final.doc - 58f6922dedb0d43c4478a4f38ad08620

July6thFinal.doc - f2a0787388dd6373336b3f23f204524a

EIDHR_action_plan.xlsx - 0fe550a5d1187d38984c505ef7741638

Dharamsala August 2012 Full program.xls - 971f99af0f9df674a79507ed7b3010fb

Each document is encrypted with a four-digit numeric password, a tactic seen previously in other emails. This tactic makes it more difficult to identify embedded payloads and the vulnerability used.

All of the files except for the first (Droeshi final.doc) have the same malware files embedded. The first uses a variant of the LURK trojan that is very similar, but not identical, to the others.

Infection

In each of the four cases, the document exploit drops the LURK trojan:

%Temp%\iexplore.exe

Two different versions of the trojan were seen between the four cases. While they all use the same filenames, in one case, the MD5 of the trojan is different:

July6thFinal.doc, EIDHR_action_plan.xlsx, Dharamsala August 2012 Full program.xls:
16160a6a9b905c69cb8e92c319212980
Droeshi final.doc: 1c22ee3326affee30c3fa65f0b8413d5

LURK also uses the following files:

Additionally, the samples that use Excel as their vector also drop a clean file, opened after the malware executes:

%AppData%\Application Data\Help\CREATELINK.EXE
%AppData%\Help\IconCacheEt.DAT
%AppData%\Help\IconConfigEt.DAT
%AppData\\Help\iexplore.exe
%Temp%\set.xls
C:\Documents and Settings\user\Start Menu\Programs\Startup\iexplore.lnk

For persistence, the trojan also creates the following link in the Startup folder, pointing at the iexplore.exe binary in %AppData%:

The binary in %AppData% is only 9KB and acts as a launcher.

IconConfigEt.DAT is the trojan's configuration file, storing the C2 server addresses and ports, as well as a campaign name identifier. The file is mostly encrypted, with the campaign name stored in the clear. The configuration options are read from the main executable using GetPrivateProfileStringW(), a function for pre-registry configuration storage. This function is for backwards compatibility with pre-registry 16-bit Windows applications, and is not commonly used in modern applications.

```
wcscat(&FileName, L"IconConfigEt.DAT");
sub_404480(&FileName);
Sleep(0x1F4u);
GetPrivateProfileStringW(L"PPP", L"P", L"NULL", (LPWSTR)ReturnedString, 0x80u, &FileName);
GetPrivateProfileStringW(L"WWW", L"W", L"NULL", (LPWSTR)WideCharStr, 0x80u, &FileName);
GetPrivateProfileStringW(L"PPP1", L"P1", L"NULL", (LPWSTR)v28, 0x80u, &FileName);
GetPrivateProfileStringW(L"WWW1", L"W1", L"NULL", (LPWSTR)v24, 0x80u, &FileName);
GetPrivateProfileStringW(L"PPP2", L"P2", L"NULL", (LPWSTR)v29, 0x80u, &FileName);
GetPrivateProfileStringW(L"WWW2", L"W2", L"NULL", (LPWSTR)v22, 0x80u, &FileName);
GetPrivateProfileStringW(L"HHH", L"H", L"NULL", (LPWSTR)&Data, 0x80u, &FileName);
sub_404560(&FileName);
for ( i = 0; i < wcslen((const wchar_t *)WideCharStr); ++i )
  --WideCharStr[i];
for ( j = 0; j < wcslen((const wchar_t *)ReturnedString); ++j )
  --ReturnedString[j];
for ( k = 0; k < wcslen((const wchar_t *)v24); ++k )
  --v24[k];
for ( l = 0; l < wcslen((const wchar_t *)v28); ++l )
  --v28[l];
for ( m = 0; m < wcslen((const wchar_t *)v22); ++m )
  --v22[m];
for ( n = 0; n < wcslen((const wchar_t *)v29); ++n )
  --v29[n];
sub_4048C0(v7, &Data);
```

Decryption of the configuration file is done in sub_4044B0() using a key generated in sub_404430() -- the default is 0x11B29719, in the case of the more common version of the trojan the key is 0x11B297A9. Once the values have been read from the decrypted file, it is re-encrypted in sub_404560().

Encrypted on disk (default):

```
00000000  87 c0 8b c0 81 9d 8b aa  b9 e2 b1 b8 b9 f8 a8 f2  |................|
00000010  f3 f9 ba 9d 87 c7 8c c7  81 9d 8c aa eb a3 d6 cc  |................|
00000020  8b c0 8b a6 81 9d 8b a6  e1 f2 a9 fa f3 f1 be e2  |................|
00000030  aa e7 f3 f3 ac f9 d6 cc  8c c7 8c a6 81 9d 8c a6  |................|
00000040  e1 a0 e8 9d 87 c0 8b c0  ee ca d6 c0 ee aa d6 cc  |................|
00000050  8c c7 8c a5 81 9d 8c a5  e1 9d 87 da 91 da 81 9d  |................|
00000060  91 aa 88 af ec a6 5b 4d  4d 4d 5d 0d 0a 4d 3d 54  |......[MMM]..M=T|
00000070  38 30 31 0d 0a                                    |801..|
00000075
```

Decrypted:

```
00000000  5b 57 57 57 5d 0d 0a 57  3d 65 75 6d 2f 65 6f 74  |[WWW]..W=eum/eot|
00000010  65 2f 6e 66 0d 0a 5b 50  50 50 5d 0d 0a 50 3d 37  |e/nf..[PPP]..P=7|
00000020  34 0d 0a 5b 57 57 57 31  5d 0d 0a 57 31 3d 65 75  |4..[WWW1]..W1=eu|
00000030  6d 2f 66 62 75 76 70 2f  64 70 6e 0d 0a 5b 50 50  |m/fbuvp/dpn..[PP|
00000040  50 31 5d 0d 0a 50 31 3d  37 34 0d 0a 5b 57 57 57  |P1]..P1=74..[WWW|
00000050  32 5d 0d 0a 57 32 3d 0d  0a 5b 50 50 50 32 5d 0d  |2]..W2=..[PPP2].|
00000060  0a 50 32 3d 0d 0a 5b 4d  4d 4d 5d 0d 0a 4d 3d 54  |.P2=..[MMM]..M=T|
00000070  38 30 31 0d 0a                                    |801..|
00000075
```

Once the configuration file is decrypted, the values are still not readable. Fortunately, the second layer decryption is an easy process -- just decrement each character by 1.

The values read from the configuration file are:

1. Section [PPP], key P: Primary C2 server port number
2. Section [WWW], key W: Primary C2 server name
3. Section [PPP1], key P1: Secondary C2 server port number
4. Section [WWW1], key W1: Secondary C2 server name
5. Section [PPP2], key P2: Tertiary C2 server port number
6. Section [WWW2], key W2: Tertiary C2 server name
7. Section [MMM], key M: Campaign name

In the configuration files we have looked at for this run, the primary server is dtl.dnsd.me:63, and the secondary server is dtl.eatuo.com:63. Both dnsd.me and eatuo.com are dynamic DNS providers, and eatuo.com has the same domain registration information as the well-known Chinese provider 3322.org. No tertiary server is given.

The malware checks in sub_4040E0() for a value of "Mark" in the registry at the following location:

```
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\DbxUpdateET\
```

If a value is not found, it is set with the campaign name read from the configuration file key M.

Campaign Names

The four samples we received use three different campaign names, identified as follows in value 7 of each configuration file:

```
Droeshi final.doc: campaign id TIBET
July6thFinal.doc: campaign id T706 (note that the password on the file is also 0706, keeping on theme)
EIDHR_action_plan.xlsx: campaign id T801
Dharamsala August 2012 Full program.xls: campaign id T801
```

The campaign names strongly suggest that these runs are specific to the Tibetan community, and that the Txxx attacks may be coming from the same source. The July6thFinal.doc, EIDHR_action_plan.xlsx, and Dharamsala August 2012 Full program.xls documents all drop the same trojan; the Droeshi final.doc trojan is slightly different (although uses much of the same code).

Malware Analysis

These samples match the behavior seen with other recorded instances of samples from this family in the wild. LURK is also known as Troj~Agent-XAT (Sophos), TROJ_MDROP.TPB and TROJ_MDROP.TPC (Trend Micro), and can also be picked up by more general antivirus detection such as Generic PWS.y (McAfee). In the sample analyzed by Sophos, the campaign ID is "IE_0day" -- not immediately related to attacks on the Tibetan community.

Many more samples within this family exist with reports online -- look for "DbxUpdateET" (where the campaign ID is stored in the registry) or the dropped files "IconCacheEt" and "IconConfigEt." Another Tibetan-themed example using the dtl.eatuo.com domain was reported by ZenLab on March 26, 2012.

The LURK malware is also referenced with a description of the communication protocol in Command Five's paper "Command and Control in the Fifth Domain." The network behavior we observed matches the described protocol.

An additional file with the T801 campaign ID that we observed used twice was uploaded to ThreatExpert and can be found here.

Command and Control Information

```
PORT STATE SERVICE VERSION
21/tcp open tcpwrapped
53/tcp open domain?
80/tcp closed http
81/tcp open hosts2-ns?
135/tcp open msrpc Microsoft Windows RPC
1026/tcp open msrpc Microsoft Windows RPC
8080/tcp open http-proxy?
```

A port scan of the C2 server shows the following ports are open:

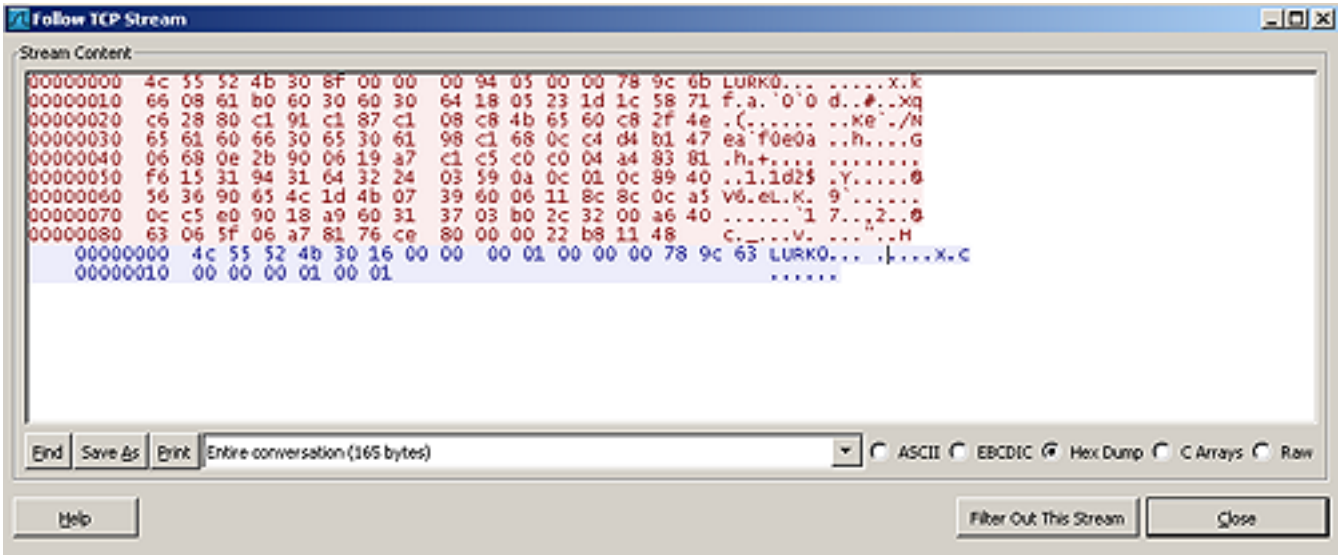
In addition to port 63 (which is not shown as open in the above scan), ports 81 and 53 are both LURK.

Network Traffic

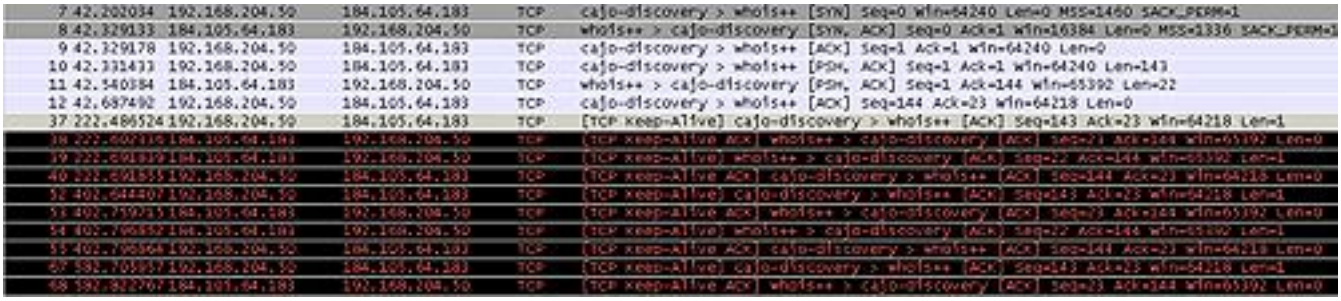
In addition to the dropped files, infected machines can be found on a network by looking for the following indications of compromise:

- DNS lookup of the C2 domains: dtl.dnsd.me, dtl.eatuo.com
- Traffic to the C2 IP: 184.105.64.183 -- this includes traffic over port 53, which is normally DNS
- TCP traffic over port 53 that begins with “LURK0”

The beginning of a network connection to the C2 server looks like this:



If the C2 is not actively responding, not much data will be transmitted beyond TCP:



For detection, Jaime Blasco from AlienVault has written a Snort rule that will detect LURK traffic (originally found here):

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"APT LURK communication protocol detected"; flow:established,to_server; content:"|4C 55 52 4B 30|"; depth:5; reference:url,www.commandfive.com/papers/C5_APT_C2InTheFifthDomain.pdf; classtype:trojan-activity; sid:3000006; rev:1;)
```

RECOMMENDATIONS

- Civil society organizations, particularly those working on issues related to Tibetan rights, should exercise caution with respect to any email containing a link or attachment. As the targeted malware attacks analyzed in this report demonstrate, content used to induce a recipient to open a malicious file may at one point have actually been authentic and private -- and is that much more likely to appear legitimate. For tips on other ways to detect probable malware attacks and prevent compromise, see Citizen Lab's Recommendations for Defending Against Targeted Cyber Threats.

- Civil society organizations should be wary of emails attaching password-protected documents and providing said password in the email body. Such purported "security" measures are not an indicator of authenticity.

- Citizen Lab encourages civil society organizations and individuals working on human rights issues that have encountered these types of targeted malware attacks to contact us at hrthreats[AT]citizenlab.org. We appreciate submission of data, which will help strengthen our analysis of cyber threats.

FOOTNOTES

[1] On April 1, 1955, the governments of India and China signed a protocol by which India handed over control of communications services in Tibet to China. See *Protocol between the Governments of India and China Regarding the Handing Over of Postal, Telegraph and Public Telephone Services in the Tibet Region of China*.

[2] The Fourteenth Dalai Lama Tenzin Gyatso was born on July 6, 1935.

[3] The Thirteenth Dalai Lama Thupten Gyatso passed away on December 17, 1933.