



The Citizen Lab

Research Brief
Number 07 – June 2012

***Spoofing the European Parliament:
An Analysis of the Repurposing of Legitimate Content
in Targeted Malware Attacks***

Part II of [Information Operations and Tibetan Rights in the Wake of Self-Immolations](#)

KEY FINDINGS

- On June 15, 2012, a malicious email with the subject “FW: the new decision of EUROPEAN PARLIAMENT about Tibetan human right in China” was sent to over 80 unique email addresses, targeting individuals active in the Tibetan rights community.
- Attached to the email is a malicious .doc file -- characterized by the email text as containing the June 14, 2012 resolution of the European Parliament on the human rights situation in Tibet -- in which is embedded malicious code that executes when the attachment is opened.
- The malware utilized in this attack is the same as that described in other reports detailing attacks with Tibet-related themes. Once the malicious code is executed, it starts to communicate with a command and control (C2) server located in Hong Kong.
- This attack raises serious questions concerning misappropriation of the intellectual property and political discourse of public entities such as the European Parliament in furtherance of information operations designed to compromise civil society organizations.
- The Citizen Lab recommends that the European Parliament and other stakeholders voice concern and engage in serious consideration and public debate regarding targeted cyber threats against civil society, which have resulted in chilling effects and information denial.

OVERVIEW

A common technique used by attackers in crafting malicious emails is to repurpose legitimate, authentic content in order to persuade a recipient to click a link or open an attachment that launches a hidden exploit. Often such content is taken from official announcements, websites of nongovernmental organizations, or publicly-available media such as news sites, and repackaged within an email that includes a malicious attachment or link. For example, malicious emails have circulated attaching content such as an [invitation to the 2010 Nobel Peace Prize ceremony](#) and [statements made in international fora](#).

Recently, attackers targeting the Tibetan community have seized on a relatively high-profile document to incorporate in targeted malware efforts: the [June 14, 2012 resolution of the European Parliament \(EP\) on the human rights situation in Tibet](#), which references the 38 Tibetan self-immolations that had occurred as of that date, and calls on the Chinese authorities to take action to respect and protect Tibetan rights.

While such a tactic is not unusual, it does raise a number of questions surrounding the use of legitimate political resources for illegitimate purposes, and the modus operandi of the attackers in this particular circumstance. Indeed, one effect (and perhaps purpose) of attacks such as this is to undermine the impact of the original content; here, an EP resolution designed to promote Tibetan rights was used as bait to compromise those very same rights, resulting in a chilling effect whereby the Tibetan community is discouraged from circulating information on the resolution, which is now associated with malware. In this report, we review some technical details of the targeted malware attack, and make recommendations regarding consideration of targeted cyber threats against civil society.

TECHNICAL ANALYSIS

On June 15, 2012, an email with the subject “FW: the new decision of EUROPEAN PARLIAMENT about tibetan human right in China” was sent to over 80 unique email addresses, targeting individuals active in the Tibetan rights community. A screenshot of the email, submitted to the Citizen Lab for analysis, is included below:

FW: the new decision of EUROPEAN PARLIAMENT about tibetan human right in China

From: tibetan welfareoffice < .com>
To:
Date: 15 Jun 2012
Subject: FW: the new decision of EUROPEAN PARLIAMENT about tibetan human right in China

Here is the new decision of EUROPEAN PARLIAMENT about tibetan human right in China, and it is so usefull for us to strive for independent nation. Please forward it to tibetan.

[signature redacted]

Attachments

- [EP joint motion for resolution - TIBET - 06.2012.doc](#)

The body of the message reads:

Here is the new decision of EUROPEAN PARLIAMENT about tibetan human right in China, and it is so usefull for us to strive for independent nation. Please forward it to tibetan.

The address in the “From” header of the email appears to be from a legitimate Tibetan organization -- likely a compromised web mail account, with the recipients of the attack perhaps coming from the account’s contact list.

It is noteworthy that, while the text of the malicious email references the European Parliament (EP) decision of June 14, the attachment itself is actually the precursor to that resolution, namely, the EP’s joint motion for resolution of June 12, 2012. The use of that document instead of the resolution proper is likely the result of the availability of that file in a prepackaged, downloadable Word document format on the [EP’s website](#); by contrast, as of June 20, 2012, the June 14 resolution was not available as a separate downloadable document, and was displayed [only in HTML](#) on the website.

Joint motion has downloadable .doc.

European Parliament

Document selected: RC-07-0312/2012

Texts labelled: RC-07-0312/2012 | Debates: OJ 12/06/2012 - 135 | Voters: PV 14/06/2012 - 11.5 | Texts adopted: P7_TA(2012)0257

JOINT MOTION FOR A RESOLUTION

12.6.2012

PE491.931(01-00) | B7-0312(2012)
 PE491.933(01-00) | B7-0314(2012)
 PE491.934(01-00) | B7-0315(2012)
 PE491.939(01-00) | B7-0319(2012)
 PE491.939(01-00) RC1 | B7-0320(2012) RC1

peruant to Rule 110(2) and (4), of the Rules of Procedure replacing the motions by the following groups:

EFD (B7-0312/2012)
 Verts/ALE (B7-0314/2012)
 ALDE (B7-0315/2012)
 PPE (B7-0319/2012)
 ECR (B7-0320/2012)

on the human rights situation in Tibet (2012/2685(RSP))

José Ignacio Salafranca Sánchez-Neyra, Thomas Mann, Ioannis Kasoulides, Filip Kaczmarek, Jarostaw Leszek Wajęsa, Roberta Angelilli, Laima Liucija Andriukienė, László Tőkés, Bernd Posselt, Cristian Dan Preda, Tunde Kristin Csaba Sógor on behalf of the PPE Group
 Kristina Oshland, Annette Heyns Gyllensboeck, Edward McMillan Scott, Marjorie Schaake, Leonidas Donskis, Ramon Tremosa i Balcells, Izaskun Bilbao Barandica, Sarah Ludford, Ivo Vajgl, Johannes Cornelis van Baalen, Jelko Kacin, Sonia Alfano, Nathalie Griesbeck, Graham Watson on behalf of the ALDE Group
 Eva Lichtenberger, Helga Trüpel, Rait Romeva i Ruuda, Nicole Kill-Andersen, Catherine Gréze on behalf of the Verts/ALE Group
 Charles Tannock, Ryszard Czarnecki, Ryszard Antoni Legutko, Tomasz Piotr Poręba on behalf of the ECR Group
 Fausto Provera on behalf of the EFD Group

European Parliament resolution on the human rights situation in Tibet (2012/2685(RSP))

The European Parliament,

- having regard to its previous resolutions on China and Tibet, in particular its resolutions of 26 October 2011⁽¹⁾ and 24 November 2010⁽²⁾,
- having regard to its previous resolution on the ban on the elections for the Tibetan government in exile in Nepal on 7 April 2011⁽³⁾,
- having regard to the Universal Declaration of Human Rights of 1948,
- having regard to Article 36 of the Constitution of the People's Republic of China, which guarantees all citizens the right to freedom of religious belief,

Resolution does not have .doc available.

European Parliament

Select a document: RC-07-0312/2012

Texts labelled: RC-07-0312/2012 | Debates: OJ 12/06/2012 - 135 | Voters: PV 14/06/2012 - 11.5 | Texts adopted: P7_TA(2012)0257

Texts adopted

Thursday, 14 June 2012 - Strasbourg

Situation in Tibet | P7_TA-PROV(2012)0257 | B7-0312, 0314, 0315, 0319 and 0320/2012

European Parliament resolution of 14 June 2012 on the human rights situation in Tibet (2012/2685(RSP))

The European Parliament,

- having regard to its previous resolutions on China and Tibet, in particular its resolutions of 27 October 2011⁽¹⁾ and 25 November 2010⁽²⁾,
- having regard to its previous resolution of 7 April 2011 on the ban on the elections for the Tibetan government in exile in Nepal⁽³⁾,
- having regard to the Universal Declaration of Human Rights of 1948,
- having regard to Article 36 of the Constitution of the People's Republic of China, which guarantees all citizens the right to freedom of religious belief,
- having regard to Rule 110(2) and (4) of its Rules of Procedure,

A. whereas respect for human rights, freedom of identity, culture, religion and association are founding principles of the EU and of its foreign policy;

B. whereas the EU raised the question of Tibetan minority rights during the 31st round of the EU-China Human Rights Dialogue held in Brussels on 29 May 2012; whereas the EU-China Human Rights Dialogue has not resulted in any significant improvements in the human rights situation of the Tibetans;

C. whereas the envoys of His Holiness the Dalai Lama have approached the Government of the People's Republic of China to find a peaceful and mutually beneficial solution to the issue of Tibet, whereas the talks between the two sides have delivered no concrete results and are currently frozen;

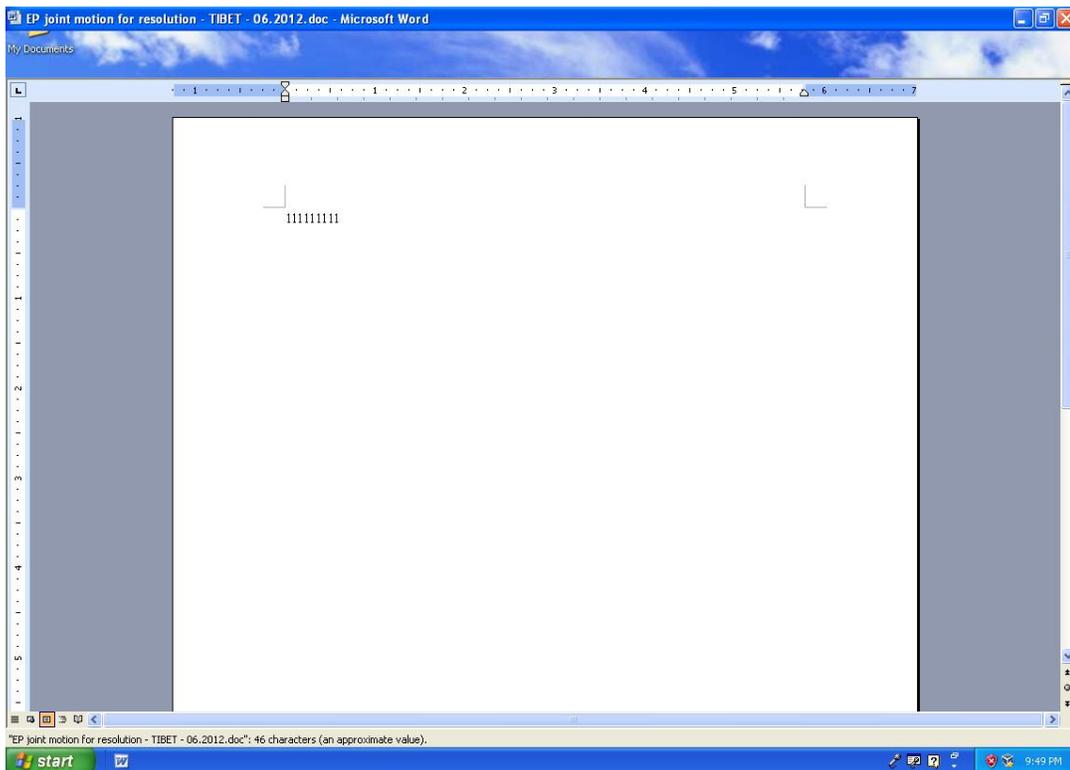
D. whereas the authorities of the People's Republic of China used disproportionate force while dealing with the protests of 2008 in Tibet and have, ever since, imposed restrictive security measures that curtail freedom of expression, freedom of association and freedom of belief;

E. whereas the number of victims of the 2008 protests may have exceeded 200, the number of those detained varies from 4 434 to more than 6 500, and there were 831 known political prisoners in Tibet at the end of 2010, of whom 360 were judicially convicted and 12 were serving life sentences;

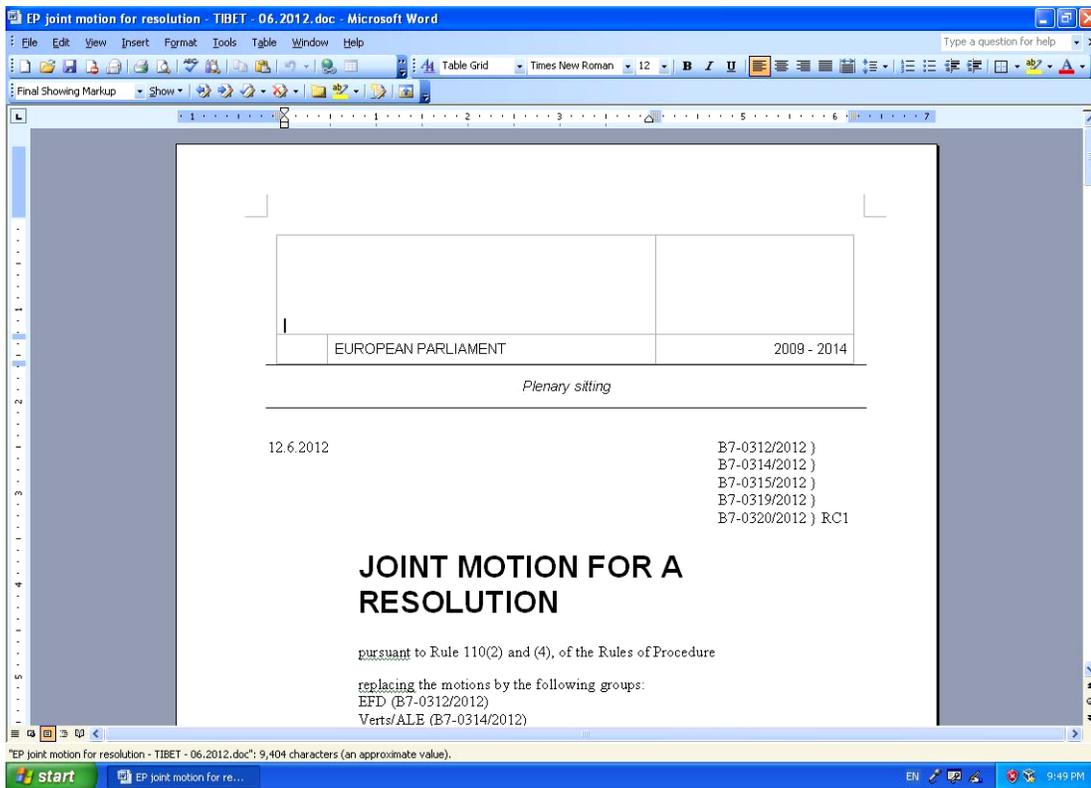
F. whereas torture, including beating, use of electroshock weapons, long-term solitary confinement, starvation and other similar measures are reportedly used to extract confessions in the prisons of Tibet by the authorities of the People's Republic of China;

G. whereas 38 Tibetans, mostly monks and nuns, have reportedly set themselves on fire since 2009 in protest against restrictive Chinese policies in Tibet and in support of the return of the Dalai Lama and the right to religious freedom in the Aba/Jigaba county prefecture in Sichuan Province and other parts of the Tibetan plateau;

The attachment to the malicious email is a Microsoft Word document titled “EP joint motion for resolution - TIBET - 06.2012.doc” with the MD5 signature 81f3a6e7a73a9845c6eb9a3d46597223. When the attachment is opened, Word briefly displays a document that contains the text “11111111” while exploiting the Microsoft Word vulnerability and dropping several files that are embedded in the attachment.



The original file then closes and Word opens a clean document (dropped in the user’s temporary directory with the same filename) that contains the full text of the joint motion for resolution, in a version that is identical in appearance to the document downloadable from the EP website.



While the file is nearly identical to the Microsoft Word file that can be downloaded from the European Parliament’s [site](#), the metadata in the documents differs in interesting ways:

Metadata	Authentic file	Dropped clean file
MD5	8882c40ef1786efb98ea251e247bfbee	40f41c077e03d72a39eb1bd7bf6e3341
Last Saved By	HSwallow	lebrale
Create Time/Date	Tue Jun 12 09:11:00 2012	Wed Jun 13 11:39:00 2012
Last Saved Time/Date	Tue Jun 12 09:11:00 2012	Wed Jun 13 11:39:00 2012

Such details suggest that the attacker was in this instance familiar with the work of the EP regarding the Tibetan human rights situation: he or she was aware of the joint motion for resolution; may have downloaded a copy of the document on June 13 (per the create time/date metadata), the day after the joint motion was released, and embedded it in the new malicious file “EP joint motion for resolution - TIBET - 06.2012.doc”; and may have held onto that file deliberately, waiting to circulate it until June 15, the day after the resolution to which it corresponds was officially adopted -- perhaps timed for when the document would attract the most interest.

As the clean file is opened, malicious code executes and communicates with a command and control (C2) server located in Hong Kong. The IP address of the C2 server is the same as the one used to send the targeted email from the web mail account: 114.142.147.51. This is a static IP address on DYXnet (a Chinese Internet service provider). The domain name vv338.com also points to this IP address; however, the malware does not perform a DNS lookup and there is no evidence that whoever registered the domain is associated with this attack.

The dropped executable code is the same as that described by [Symantec in a May 24, 2012 blog post](#), which details a targeted attack also incorporating Tibet-related themes. The exact filename of the original dropped executable is different (NvDev.exe instead of NvSmart.exe), and was likely changed to avoid antivirus detection. The program has a valid digital signature because it is a legitimate program, which loads and calls code from a companion DLL (dynamic link library). In this case, the attackers have provided a fake DLL which contains the malicious code. This technique, known as “DLL Hijacking,” bypasses warnings that a program is not digitally signed -- which may be a warning to the user that something is not right.

Below are screenshots of the payload code (in the malware referencing the EP resolution, in BOOT.LDR; in the malware from the Symantec post, loaded from an executable). Aside from the addresses being different, the code is the same.

Code dropped by the [HHDLschedule.doc](#) malware described by Symantec.

```

seg000:00026910      push  ebp
seg000:00026911      mov   ebp, esp
seg000:00026913      mov   eax, fs:dword_30
seg000:00026919      mov   eax, [eax+0Ch]
seg000:0002691C      mov   eax, [eax+1Ch]
seg000:0002691F      sub   esp, 100h
seg000:00026925      push  ebx
seg000:00026926      push  esi
seg000:00026927      xor   ebx, ebx
seg000:00026929      loc_26929:                ; CODE XREF: sub_26910+26jj
seg000:00026929      cmp   dword ptr [eax+1Ch], 1A0018h
seg000:00026930      jz   short loc_2693A
seg000:00026932      mov   eax, [eax]
seg000:00026934      cmp   eax, ebx
seg000:00026936      jnz  short loc_26929
seg000:00026938      jmp  short loc_26941
seg000:0002693A      ;
seg000:0002693A      loc_2693A:                ; CODE XREF: sub_26910+20fj
seg000:0002693A      mov   esi, [eax+8]
seg000:0002693D      cmp   esi, ebx
seg000:0002693F      jnz  short loc_26949
seg000:00026941      loc_26941:                ; CODE XREF: sub_26910+28fj
seg000:00026941      xor   eax, eax
seg000:00026943      inc  eax
seg000:00026944      jmp  loc_26EC2
seg000:00026949      ;
seg000:00026949      loc_26949:                ; CODE XREF: sub_26910+2Ffj
seg000:00026949      mov   eax, [esi+3Ch]
seg000:0002694C      mov   ecx, [eax+esi+78h]
seg000:00026950      add  ecx, esi
seg000:00026952      mov   edx, [ecx+20h]
seg000:00026955      push  edi
seg000:00026956      add  edx, esi
seg000:00026958      xor  edi, edi
seg000:0002695A      cmp  [ecx+18h], ebx
seg000:0002695D      jle  short loc_269C1
seg000:0002695F      loc_2695F:                ; CODE XREF: sub_26910+93jj
seg000:0002695F      mov  eax, [edx+edi*4]
seg000:00026962      add  eax, esi
seg000:00026964      cmp  byte ptr [eax], 47h ; 'G'

```

Code dropped by the “EP joint motion for resolution - TIBET - 06.2012.doc” document.

```

seg000:0001CA2B      push  ebp
seg000:0001CA2C      mov   ebp, esp
seg000:0001CA2E      mov   eax, fs:dword_30
seg000:0001CA34      mov   eax, [eax+0Ch]
seg000:0001CA37      mov   eax, [eax+1Ch]
seg000:0001CA3A      sub   esp, 100h
seg000:0001CA40      push  ebx
seg000:0001CA41      push  esi
seg000:0001CA42      xor   ebx, ebx
seg000:0001CA44      ;
seg000:0001CA44      loc_1CA44:                ; CODE XREF: sub_1CA2B+26jj
seg000:0001CA44      cmp   dword ptr [eax+1Ch], 1A0018h
seg000:0001CA48      jz   short loc_1CA55
seg000:0001CA4D      mov   eax, [eax]
seg000:0001CA4F      cmp   eax, ebx
seg000:0001CA51      jnz  short loc_1CA44
seg000:0001CA53      jmp  short loc_1CA5C
seg000:0001CA55      ;
seg000:0001CA55      loc_1CA55:                ; CODE XREF: sub_1CA2B+20fj
seg000:0001CA55      mov   esi, [eax+8]
seg000:0001CA58      cmp   esi, ebx
seg000:0001CA5A      jnz  short loc_1CA64
seg000:0001CA5C      loc_1CA5C:                ; CODE XREF: sub_1CA2B+28fj
seg000:0001CA5C      xor   eax, eax
seg000:0001CA5E      inc  eax
seg000:0001CA5F      jmp  loc_1CFD0
seg000:0001CA64      ;
seg000:0001CA64      loc_1CA64:                ; CODE XREF: sub_1CA2B+2Ffj
seg000:0001CA64      mov   eax, [esi+3Ch]
seg000:0001CA67      mov   ecx, [eax+esi+78h]
seg000:0001CA68      add  ecx, esi
seg000:0001CA6D      mov   edx, [ecx+20h]
seg000:0001CA70      push  edi
seg000:0001CA71      add  edx, esi
seg000:0001CA73      xor  edi, edi
seg000:0001CA75      cmp  [ecx+18h], ebx
seg000:0001CA78      jle  short loc_1CADC
seg000:0001CA7A      loc_1CA7A:                ; CODE XREF: sub_1CA2B+93jj
seg000:0001CA7A      mov  eax, [edx+edi*4]
seg000:0001CA7D      add  eax, esi
seg000:0001CA7F      cmp  byte ptr [eax], 47h ; 'G'

```

RECOMMENDATIONS

This attack demonstrates the ease of repurposing legitimate content in a manner that is likely to appear authentic to, and prompt the interest of, the intended target of the malware. It also raises serious questions concerning misappropriation of the intellectual property and political resources of public entities -- in this case, utilizing an EP resolution to compromise the Tibetan community, the very individuals the EP, on behalf of European citizens, sought to protect.

The Citizen Lab recommends:

- That members of the Tibetan community and others concerned with Tibetan rights exercise caution concerning “official” documents circulated as attachments, including those referencing the June 14 EP resolution (for tips on preventing exposure to malware, see the Citizen Lab’s [Recommendations for Defending Against Targeted Cyber Threats](#));
- That the European Parliament, in light of this recent example of malware attacks incorporating the EP’s own work in order to target human rights organizations and activists, voice its concern publicly about this incident. The Citizen Lab also recommends that the EP engage in serious consideration and public debate regarding targeted cyber threats against civil society in general; and
- That policy and technical communities engage in closer collaboration and discussion of the threats that are now increasingly common against civil society in cyberspace, and work to identify measures to proactively defend against and mitigate such threats.