Citizen Lab, Munk School of Global Affairs, University of Toronto

MUNK SCHOOL OF GLOBAL AFFAIRS

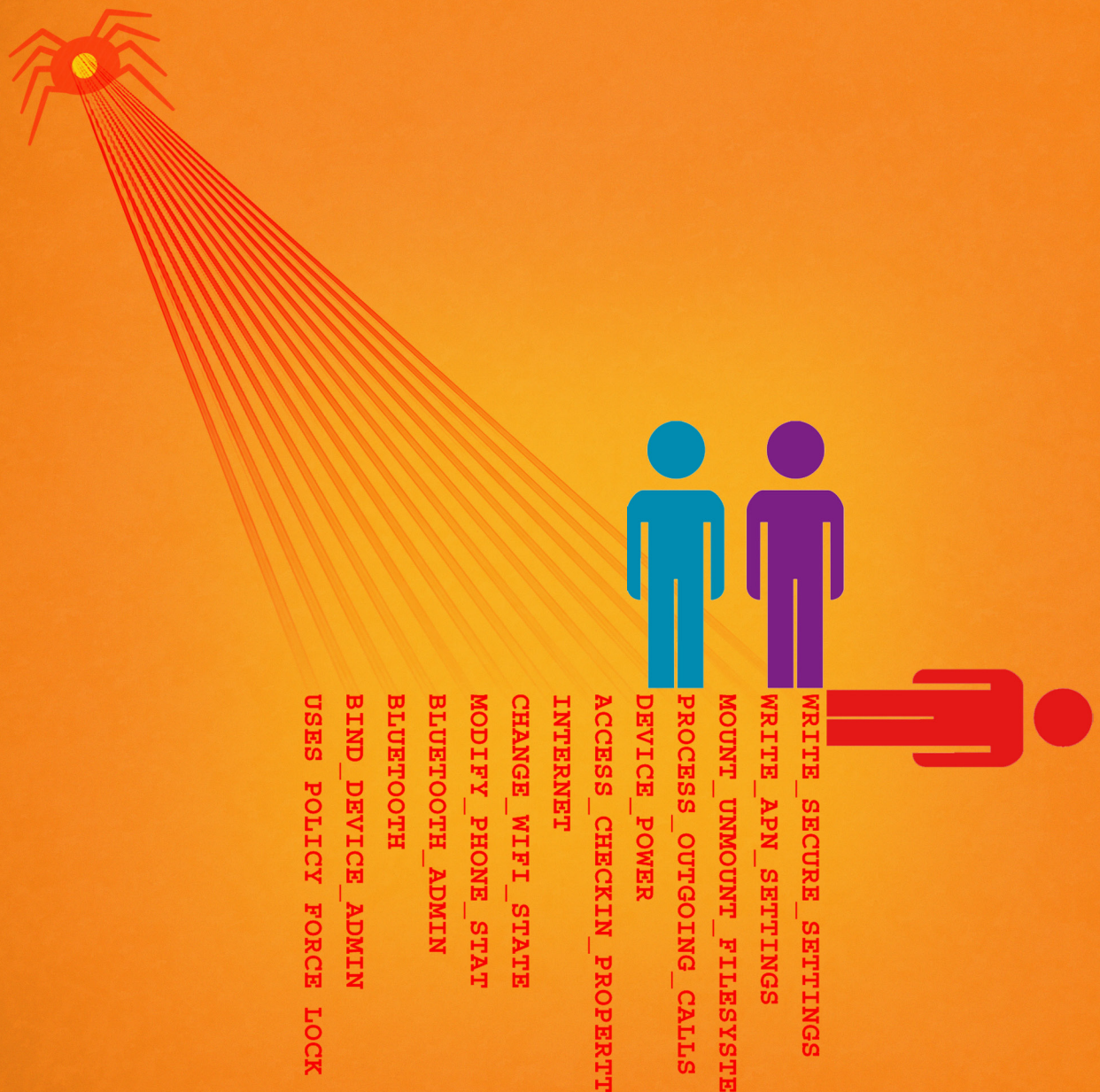
UNIVERSITY OF TORONTO

COMMUNITIES @ RISK

Targeted Digital Threats Against Civil Society

November 11, 2014

https://targetedthreats.net/



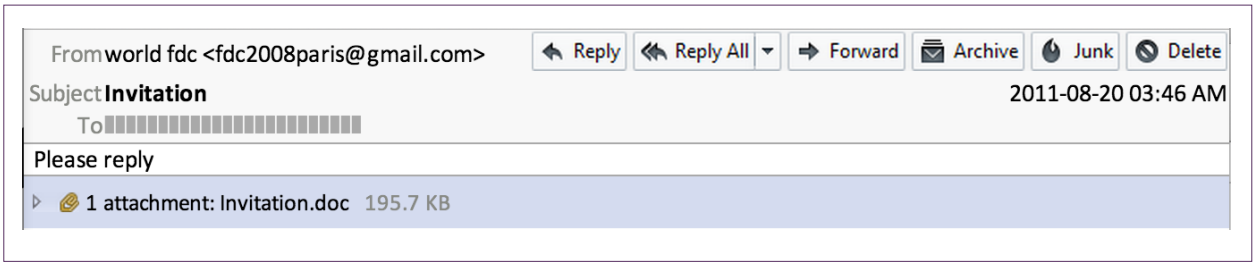
Appendix A:

Social Engineering Sophistication Score Examples

In this section, we provide specific examples of emails that would be assigned targeting scores described in The Extended Analysis.

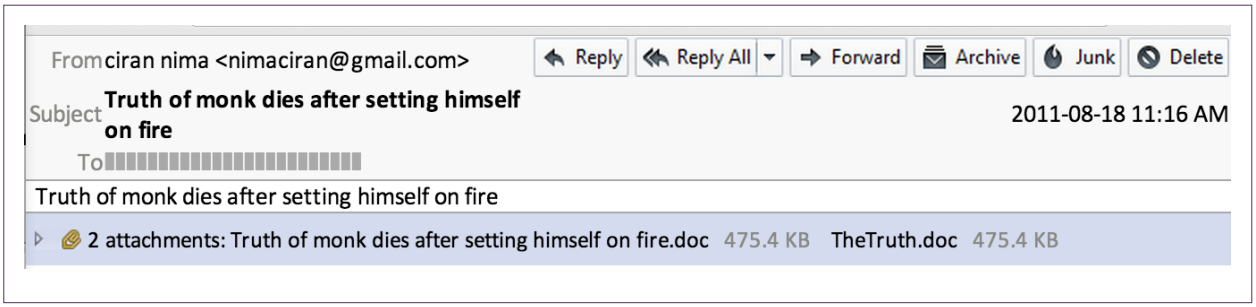
Social Engineering Sophistication Score 1 (Targeted, Not Customized)

This email was sent to Tibet Group 1. The message content and sender are vague and do not relate to the interest of the group. The attachment is a Word document implanted with malware. The lack of relevant information in this message gives it a score of 1 (Targeted, Not customized).



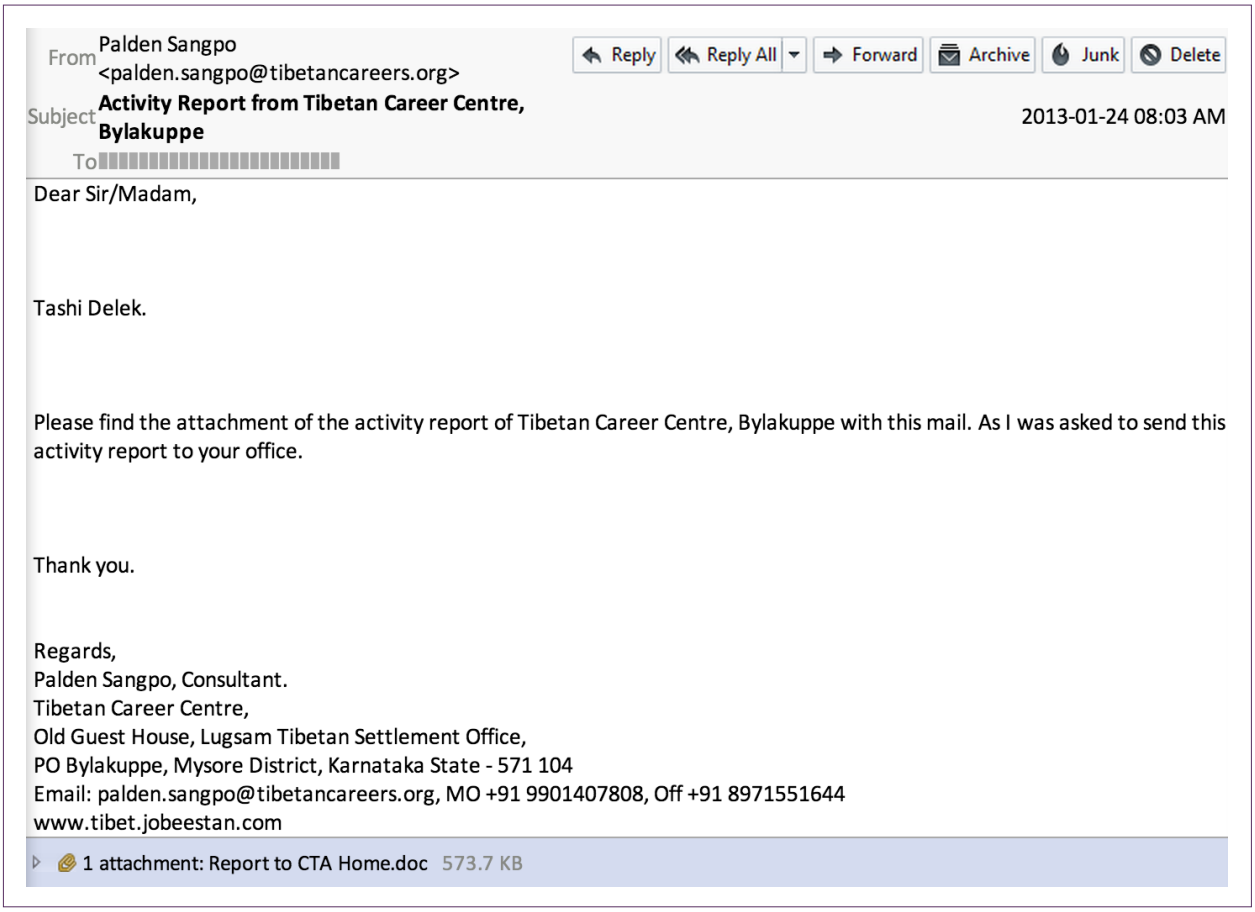
Social Engineering Sophistication Score 2 (Targeted, Poorly Customized)

This email was sent to Tibet Group 1. It references Tibetan self-immolations, an issue of interest to the group. However, the sender does not appear to be a real person or organization and the message content is terse and does not reference information that can be externally validated. While this message references content relevant to the recipient, it does not appear to come from a real person or organization, or repurpose externally verifiable content, and therefore scores a 2 (Targeted, Poorly Customized).



Social Engineering Sophistication Score 3 (Targeted, Customized)

This email was sent to Tibet Group 2. On the surface it appears to be a professional email from "Palden Sangpo," a consultant at the Tibet Career Centre. The email sender address and signature reference accurate contact details that can be easily verified through an Internet search. However, inspection of the email headers reveals the purported email sender address is fraudulent and the actual sender was albano_kuqo@gmx.com. The email generally addresses the organization, rather than the individual recipient. Therefore, this message scores a 3 (Targeted, Customized).



From: Palden Sangpo <palden.sangpo@tibetancareers.org>
Reply | Reply All | Forward | Archive | Junk | Delete
Subject: **Activity Report from Tibetan Career Centre, Bylakuppe**
2013-01-24 08:03 AM
To: [redacted]

Dear Sir/Madam,

Tashi Delek.

Please find the attachment of the activity report of Tibetan Career Centre, Bylakuppe with this mail. As I was asked to send this activity report to your office.

Thank you.

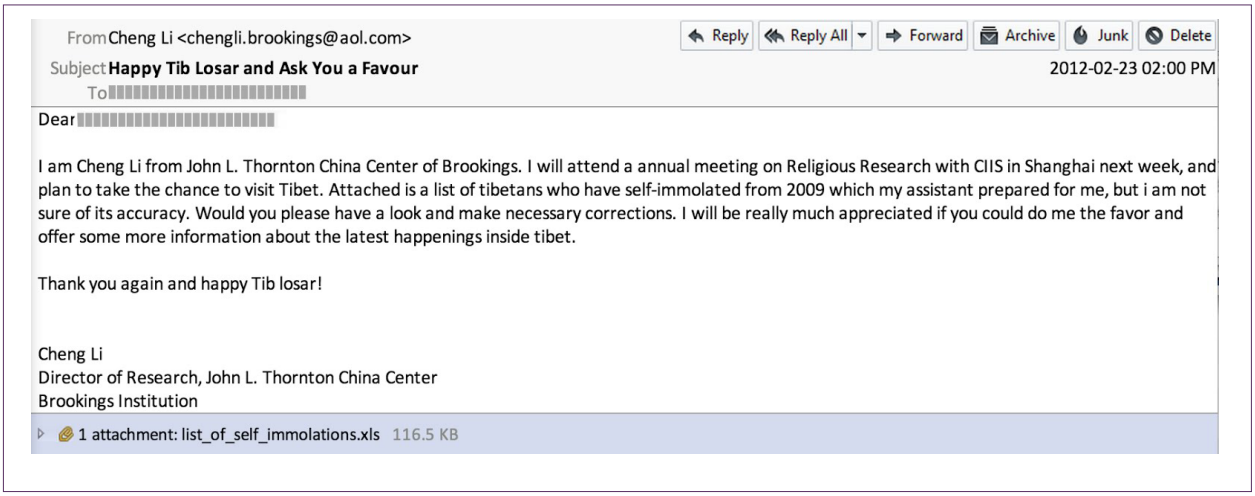
Regards,
Palden Sangpo, Consultant.
Tibetan Career Centre,
Old Guest House, Lugsam Tibetan Settlement Office,
PO Bylakuppe, Mysore District, Karnataka State - 571 104
Email: palden.sangpo@tibetancareers.org, MO +91 9901407808, Off +91 8971551644
www.tibet.jobeestan.com

1 attachment: Report to CTA Home.doc 573.7 KB

Social Engineering Sophistication Score 4 (Targeted, Personalized)

This email sent to Tibet Group 1 is directly addressed to the director of the group and purports to come from Cheng Li, a prominent China scholar based at the Brookings Institution. The message asks the recipient for information on recent Tibetan self-immolations. The email

address is made to appear to be from Cheng Li, but is actually sent from an AOL account (chengli.brookings@aol.com) that was registered by the attackers. The level of customization and personalization used in this message gives it a score of 4 (Targeted, Personalized).



Social Engineering Sophistication Score 5 (Targeted, Highly Personalized)

Targeting scores of 5 (Targeted, Highly Personalized) require use of internal information from the target organization that could not be obtained through open sources. For example, Tibet Group 2 and Tibet Group 3 received separate emails that contained specific personal details about a South African group's visit to Dharamsala, India that appear to have been repurposed from a real private communication. The email was written as a request to the Tibetan organizations for help with the planned trip. The malicious attachment contains an authentic travel itinerary, which would be displayed after the user opens the document and becomes infected by the malware. The private information used in these messages suggests that the attackers likely obtained it through a prior compromise of the group's communications.