UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

The Citizen Lab

Research Brief
October 2013

Targeted Threats Index

Author: Seth Hardy

INTRODUCTION

The Targeted Threat Index is a metric for assigning an overall threat ranking score to email messages that deliver malware to a victim's computer. The TTI metric was first introduced at SecTor 2013 by Seth Hardy as part of the talk "RATastrophe: Monitoring a Malware Menagerie" along with Katie Kleemola and Greg Wiseman.

In Citizen Lab's ongoing analysis of targeted attacks against human rights organizations, we have seen a wide range of threats varying in level of both social engineering and technical complexity. While other scoring systems exist for the purpose of communicating the level of severity and danger of a vulnerability, no common system exists for ranking the sophistication of targeted email attacks. This gap is likely because evaluating the sophistication of the targeting is non-technical, and can't be automated due to the requirement of a strong familiarity with the underlying subject material.

The TTI score is calculated by taking a base value determined by the sophistication of the targeting method, which is then multiplied by a value for the technical sophistication of the attachment. The base score can be used independently to compare emails, and the combined score gives an indication of how much work an attacker is putting into individual threats.

The TTI score is intended for use in prioritizing the analysis of incoming threats, as well as for getting an overall idea of how severely an organization is threatened.

TTI METRIC

The TTI score is calculated in two parts:

*(Targeting Sophistication Base Value) * (Technical Sophistication Multiplier) = TTI Score*

For targeted threats, final TTI scores range from 1 to 10, where 10 is the most sophisticated attack. Scores of 0 are reserved for threats that are not targeted, even if they are malicious. For example, spam using an attached

PDF or XLS to bypass anti-spam filters, and highly sophisticated financially motivated malware, would both score 0.

TARGETING SOPHISTICATION - BASE VALUE

The base value of the score ranges from 0 to 5, based on the sophistication of the email's social engineering techniques used to get the victim to open the attachment. This score considers the content and presentation of the message as well as the claimed sender identity. This determination also includes the content of any associated files; many times malware is injected into legitimate relevant documents.

Value	Description
0	Not targeted, e.g. spam or financially motivated malware.
1	Targeted but not customized. Sent with a message that is obviously false with little to no validation required.
2	Targeted and poorly customized. Content is generally relevant to the target. May look questionable.
3	Targeted and customized. May use a real person/organization or content to convince the target the message is legitimate. Content is specifically relevant to the target and looks legitimate.
4	Targeted and well-customized. Uses a real person/organization and content to convince the target the message is legitimate. Probably directly addressing the recipient. Content is specifically relevant to the target, looks legitimate, and can be externally referenced (e.g. by a website). May be sent from a hacked account.
5	Targeted and highly customized using sensitive data. Individually targeted and customized, likely using inside/sensitive information that is directly relevant to the target.

Table 1: TTI Base Value Score

Higher scores rely on detailed knowledge of personal details about the recipient and their field, including trust networks between organizations. Among the highest scoring emails include those sent with insider knowledge from internal business meetings, strongly suggesting that someone within the organization has already been compromised. Slightly lower scoring emails have included one organization in our study receiving information claiming to be from another participating organization - members of either organization would be able to immediately identify the email as suspicious.

TECHNICAL SOPHISTICATION - MULTIPLIER

The technical sophistication score is a multiplier ranging from 1 to 2 based on how advanced the associated malware is, including malicious file attachments as well as links to malware hosted on another system. We use a multiplier because advanced malware requires significantly more effort and time (or money, in the case of commercial solutions) to custom-tune for a particular target.

In this section, "associated malware" refers to the payload of the malware, and not to the exploit used to get it on the victim's computer. Malware features that increase the sophistication may not reduce detection by AV (anti virus) software if used alongside an old exploit or one that is easy to detect. Likewise, a 0-day exploit may be used to carry malware that is easily picked up by a desktop AV scanner, although this is very unlikely. AV detection rates are not directly tied to technical sophistication, and should not be used to determine multiplier value without analysis of the underlying code.

Value	Description
1	The sample contains no code protection such as packing, obfuscation (e.g. simple rotation of C2 names or other interesting strings), or anti-reversing tricks.
1.25	The sample contains a simple method of protection, such as one of the following: code protection using publicly available tools where the reverse method is available, such as UPX packing; simple anti-reversing techniques such as not using import tables, or a call to IsDebuggerPresent(); self-disabling in the presence of AV software.
1.5	The sample contains multiple minor code protection techniques (anti-reversing tricks, packing, VM / reversing tools detection) that require some low-level knowledge. This level includes malware where code that contains the core functionality of the program is decrypted only in memory.
1.75	The sample contains minor code protection techniques along with at least one advanced protection method such as rootkit functionality or a custom virtualized packer.
2	The sample contains multiple advanced protection techniques, e.g. rootkit capability, virtualized packer, multiple anti-reversing techniques, and is clearly designed by a professional software engineering team.

Table 2: TTI Technical Sophistication Multiplier

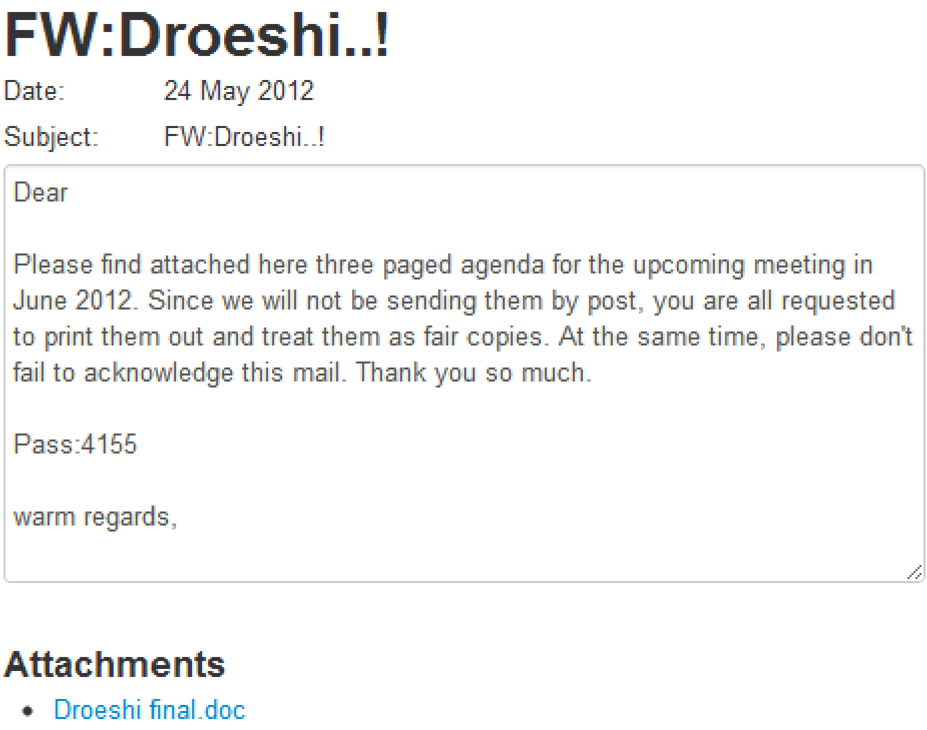
Almost all submitted samples we have analyzed have a technical sophistication multiplier of 1.5 or less, with exceptions of commercial malware such as FinFisher and DaVinci, both of which would score 2.

EXAMPLES

Here we will review the four emails described in our blog post from July 26, 2012: Recent Observations in Tibet-Related Information Operations: Advanced social engineering for the distribution of LURK malware.

In each of these cases, the malware payload is a variant of Gh0st RAT using the LURK0 flag text. Gh0st RAT is well-known and has been extensively analyzed; its technical sophistication is 1.25 for the limited protection techniques it uses.

“Droeshi” Targeting Sophistication: **3/5** Technical Sophistication: **1.25/2** TTI Score: **3.75/10**



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

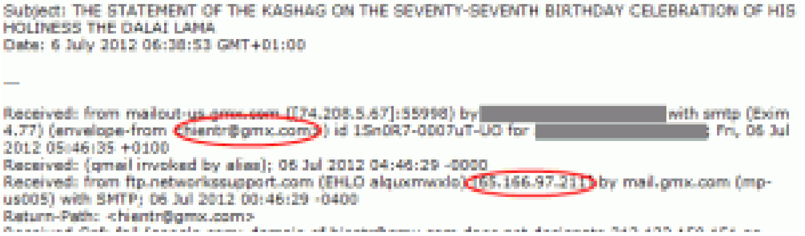
This email was sent from what appears to be a compromised account of a Tibetan activist, and does not include a named recipient or sender. The malicious attachment also does not contain any content for social engineering purposes.

While the content of the message is vague, the password and the sender name/address (not shown here for confidentiality reasons) are enough to demonstrate targeting customization.

“Statement of the Kashag” Targeting Sophistication: **2/5** Technical Sophistication: **1.25/2** TTI Score: **2.5/10**

This email, with the subject “THE STATEMENT OF THE KASHAG ON THE SEVENTY-SEVENTH BIRTHDAY CELEBRATION OF HIS HOLINESS THE DALAI LAMA”, claims to be from a real Tibetan organization. The only content of the email is a password based on the content of the email that would be easily recognizable by Tibetans: the birthday of the Dalai Lama.

While the content is relevant, this email is more questionable than the previous one. In addition to the lack of email body content, it is pretty clear to the trained eye that the From: email address was forged:

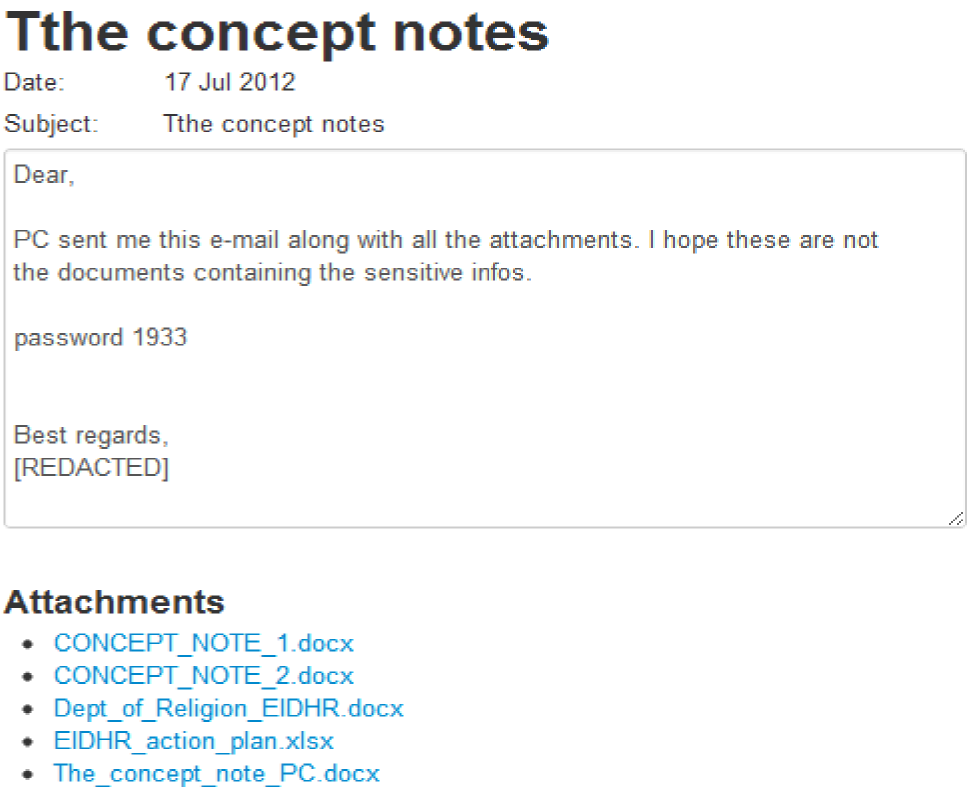


```
Subject: THE STATEMENT OF THE KASHAG ON THE SEVENTY-SEVENTH BIRTHDAY CELEBRATION OF HIS
HOLINESS THE DALAI LAMA
Date: 6 July 2012 06:38:53 GMT+01:00

—

Received: from mailout-us.gmx.com ([74.208.5.67]:55998) by [redacted] with smtp (Exim
4.77) (envelope-from <chientr@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) [65.166.97.21] by mail.gmx.com (mp-
us005) with SMTP; 06 Jul 2012 00:46:29 -0400
Return-Path: <chientr@gmx.com>
```

“The concept notes” Targeting Sophistication: **1/5** Technical Sophistication: **1.25/2** TTI Score: **1/10**

The third email of this group claims to be from a representative of the Office of Tibet, but is very vague in wording and has a number of attachments. While the malicious Excel file claiming to be related to the The European Instrument for Democracy and Human Rights (EIDHR) call for proposal is relevant, it is also in an incorrect file format (Excel OLE, and not the Open XML format the .xlsx extension claims to be) that will not open as-is. Requiring manual changing of the file name is a very strong warning sign that something is wrong.

One of the emails was even misspelled:



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

:

For all of these warning signs, this email scores very low, even though the malware included is the same.

"August visit of South African group" Targeting Sophistication: **5/5** Technical Sophistication: **1.25/2** TTI Score: **6.25/10**

The last of the LURK0 emails contains very specific personal details about a group's visit to Dharamsala, and appears to have been stolen and repurposed from a genuine conversation. The email is written as a request to the Tibetan organization for help, describing the trip. The malicious attachment contains an authentic itinerary, which is displayed after the victim is infected.

For being a well-written email that is in many ways as legitimate as it can be, and requires inside information, this email scores 5 out of 5.

TTI SCORES AND STUDY DATA

Plotting the TTI targeting score for all of the samples we have received as part of the study gives an idea of how frequently advanced targeting methods are used. In total we are working with 10 different human rights organizations. Eight of these groups focus on China-related rights issues (categorized as "China Groups). Five of those groups focus primarily on Tibetan rights (categorized as "Tibet Groups"). The remaining two focus on a variety of human rights issues (categorized as “Rights Groups”).

Out of 750 email threats received, only five score a full 5/5 on the TTI targeting base value. However, well customized email lures (targeting scores 3-4) are common. The majority of our submissions have come from Tibetan organizations.

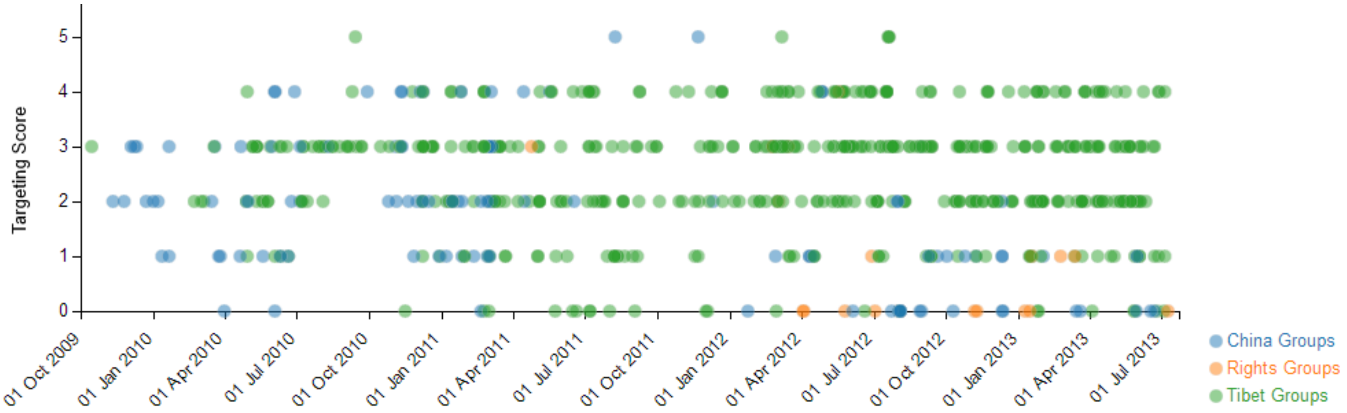


Figure 1: TTI Base Targeting Score For All Email Submissions

As there is less variance on the technical multiplier as there is on the targeting base value, the score clusters are still present in the full TTI score. Even without technically superior malware such as FinFisher, high TTI scores are still possible when an attacker cares enough to steal and use insider information as part of the attack.

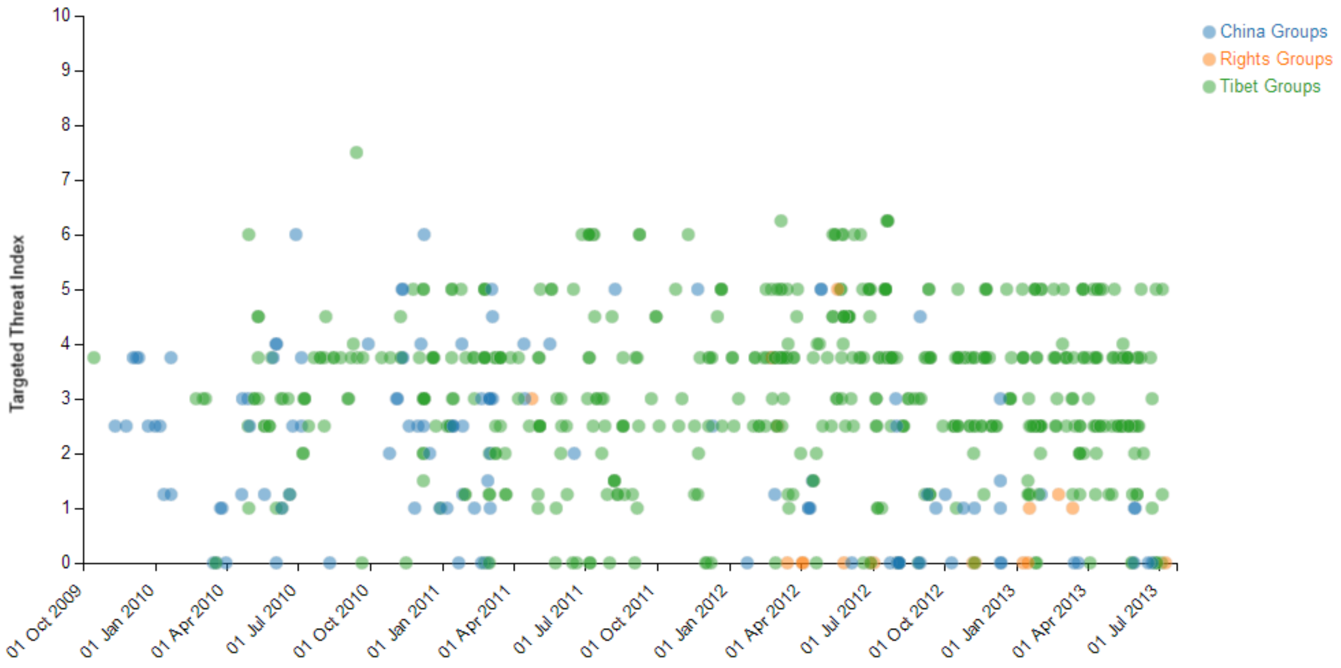


Figure 2: TTI Score For All Email Submissions

Out of the 750 submissions, 599 emails have been assigned a score greater than zero.

Mean targeting base score: **2.6**   Median targeting base score: **3.0**

Mean technical multiplier: **1.24** Median technical multiplier: **1.25**

Mean TTI: **3.23** Median TTI: **3.0**

LIMITATIONS

The Targeted Threat Index is currently a test metric, but it does give insight into the distribution of how sophisticated the threats are. As we build up a greater collection of scored samples, including those from other groups and public repositories such as Contagio, areas for revision may appear.

Average TTI scores in our case may be skewed due to the self-reporting method we use in the study. Very good threats are less likely to be noticed and reported while being sent to far fewer people, and low-quality emails are much more likely to be sent in bulk and stand out. We are more interested, however, in worst-case (highest) scores and not in comparing the average threat severity between organizations.

Finally, this metric is calculated based on the technical sophistication of the payload, not on the exploit. There is currently no method to modify the TTI score in a way similar to the temporal metrics used by the CVSS metric. A temporal metric could be added to increase the final TTI value for 0-day vulnerabilities, or possibly to reduce the score for exploits that are easily detectable due to a public and well-known generation script, e.g. Metasploit.

About The Author

Seth Hardy is a Senior Security Analyst at the Citizen Lab, Munk School of Global Affairs, University of Toronto. Prior to the Citizen Lab, he worked for a large anti-virus vendor. Seth has worked extensively on analysis of document-based malware and AV evasion methods. Other areas of experience include: provably secure cryptography, random number generators, and network vulnerability research. Seth has spoken at a number of security conferences including Black Hat, DEF CON, SecTor, and the CCC. He holds degrees from Worcester Polytechnic Institute in Mathematics and Computer Science.