- SIDtoday Article
- Letter to the Editor
- SIGINT-y Social Media Page

**(TS//SI//REL) Who Else Is Targeting Your Target? Collecting Data Stolen by Hackers**

FROM: (U//FOUO) Menwith Hill Station (F77)

Run Date: 05/06/2010

(TS//SI//REL) Hackers are stealing the emails of some of our targets... by collecting the hackers' "take," we 1) get access to the emails themselves and 2) get insights into who's being hacked.

(TS//SI//REL) People who open attachments from unknown senders (gasp) or respond to "Nigerian" money laundering emails aren't the only individuals on the internet being hacked. Some of ***our*** targets are also being targeted by outside forces, both by state-sponsored and freelance hackers. Could your target's communications be the target of other countries or groups?

(TS//SI//REL) Recently, Communications Security Establishment Canada (CSEC) and Menwith Hill Station (MHS) discovered and began exploiting a target-rich data set being stolen by hackers. The hackers' sophisticated email-stealing intrusion set is known as INTOLERANT. Of the traffic observed, nearly half contains category hits because the attackers are targeting email accounts of interest to the Intelligence Community. Although a relatively new data source, TOPIs have already written multiple reports based on INTOLERANT collect.

(U) **Technique**

(TS//SI//REL) To the analyst using SIGINT databases, collected INTOLERANT data looks like Simple Mail Transfer Protocol (SMTP) mail. In this case, though, the traffic fairy has been hard at work... To hide the traffic, the hackers' programs split a victim's email into pieces. Each piece is then obfuscated, given a different, spoofed, source IP address and sent to a different destination IP address. Having different destination IP addresses serves to route the pieces across separate channels[1] of a satellite signal. The channels being used carry large amounts of traffic, allowing INTOLERANT data to hide as background noise. Much collaboration between CSE, MHS, GCHQ and NSAW has brought about the transformation of INTOLERANT data we collect into "readable" SMTP mail.

(U//FOUO) **Victim Set**

(TS//SI//REL) INTOLERANT traffic is very organized. Each event is labeled to identify and categorize victims. Cyber attacks commonly apply descriptors to each victim - it helps herd victims and track which attacks succeed and which fail. Victim categories make INTOLERANT interesting:

A = Indian Diplomatic & Indian Navy
B = Central Asian diplomatic
C = Chinese Human Rights Defenders
D = Tibetan Pro-Democracy Personalities
E = Uighur Activists
F = European Special Rep to Afghanistan and Indian photo-journalism
G = Tibetan Government in Exile

(TS//SI//REL) New victims appear to flood out their entire inbox, going back months or, even, years. Then only new mail is transmitted. Hundreds of emails are seen on an average day.

(U) **Attribution**

(TS//SI//REL) Within the world of cyber exploitation, attribution is always difficult and INTOLERANT is no exception. Initial analysis points toward a likely state sponsor based on the level of sophistication and the victim set. Determining which state is sponsoring the activity has yet to be done. Since the traffic is traveling over satellite, the culprit must be within the satellite beam's footprint to receive the stolen emails. There was hope the footprint would point to which state was responsible, but that hope was not realized as shown in the image.

*(TS//SI//REL) Attribution of INTOLERANT data is difficult, since the satellite beam footprint is so large. Eventually, the virtual team working this effort would like to know who is hacking whom.*

(U) **Way Forward**

(TS//SI//REL) Analysis continues with the goal of learning more about the attacks as well as improving attribution. Efforts are also being made to inform relevant parties, including NTOC, due to the obvious operations security (OPSEC) concerns where US and UK authorities have contact with Indian diplomats or the European Special Representative, for instance.

(TS//SI//REL) ***So the next time you scan your target's email, pay special attention to the case notation.*** If it contains 4PXFIL[2] (E9BDJ4PXFIL.targetNumber in the case of INTOLERANT), then the email is likely available because somebody else has hacked your target. For additional details, send an email to mhsindex@nsa.ic.gov.

(U//FOUO) POCs: [REDACTED]; INDEX team (MHS)

(U) Notes:

1. (U//FOUO) Packet Identifiers, PIDs are used in satellite hub signals to designate sub-channels.

2. (TS//SI//REL) 4PXFIL stands for "fourth party exfil" or "out-sourcing SIGINT." These terms are used within the SIGINT community to refer to the practice of collecting data as it transits the Internet going from the victim's computer to the attacker's.

*(U//FOUO) SIDtoday editor's note: This article is reprinted from MHS's Horizon newsletter, March edition.*

Comments/Suggestions about this article?


Information Owner: [REDACTED] Page Publisher: [REDACTED]
Last Modified: 11/10/2012 / Last Reviewed: 11/10/2012