SID Today

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

2. (TS//SI//REL) 4PXFIL stands for "fourth party exfil" or "out-sourcing SIGINT." These terms are used within the SIGINT community to describe the practice of collecting data as it transits the Internet going from the victim's computer to the attacker. The hackers' sophisticated coding hiding techniques are known as INTOLERANT. Of the traffic observed, nearly half contains category hits because the attackers are targeting e-mail accounts of interest to the Intelligence Community. Although a relatively new data source, INTOLERANT traffic is very organized. Each event is labeled to identify and categorize victims. Cyberspace attackers commonly apply description to each victim – often hurling their victim to distinguish them from other attack victims. Victim categories make INTOLERANT interesting:

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

(TS//SI//REL) INTOLERANT traffic is very organized. Each event is labeled to identify and categorize victims. Cyberspace attackers commonly apply description to each victim – often hurling their victim to distinguish them from other attack victims. Victim categories make INTOLERANT interesting:

(TS//SI//REL) INTOLERANT data looks like Simple Mail Transfer Protocol (SMTP) email. In this case, though, the traffic sent has been shown to work. To hide the traffic, the hackers' program splits e-mails into pieces. Each piece is then reassembled, given a different source IP address and sent to a different destination IP address. Having different destination IP addresses serves to route the pieces across separate channels of a satellite signal. The channels being used carry large amounts of traffic, allowing INTOLERANT data to hide in background noise. Much collaboration between CSE, MHS, and NSA has brought about the transformation of INTOLERANT data we collect into "readable" SMTP mail.

(TS//SI//REL) If an attacker manages to capture the e-mail's source IP address, then the e-mail is likely available because somebody else has hacked your target. For additional details, send an email to mhsindex@nsa.ic.gov.

(TS//SI//REL) Attribution of INTOLERANT data is difficult, since the virtual footprint is so large. Occasionally, the virtual source e-mail domain is known where US and UK authorities have contact with Indian diplomats or the European Special Representative, for instance.

(TS//SI//REL) Attribution of INTOLERANT data is difficult, since the virtual footprint is so large. Occasionally, the virtual source e-mail domain is known where US and UK authorities have contact with Indian diplomats or the European Special Representative, for instance.

(TS//SI//REL) INTOLERANT is the first time an e-mail sent to your target's email will pay special attention to the case notation. If an email contains INTOLERANT spam, it's likely that something is afoot. The point is to learn what's going on and what's being hacked. For additional details, send an email to mhsindex@nsa.ic.gov.

(TS//SI//REL) INTOLERANT is the first time an e-mail sent to your target's email will pay special attention to the case notation. If an email contains INTOLERANT spam, it's likely that something is afoot. The point is to learn what's going on and what's being hacked. For additional details, send an email to mhsindex@nsa.ic.gov.

(TS//SI//REL) INTOLERANT's traffic is very organized. Each event is labeled to identify and categorize victims. Cyberspace attackers commonly apply description to each victim – often hurling their victim to distinguish them from other attack victims. Victim categories make INTOLERANT interesting:

(TS//SI//REL) INTOLERANT's traffic is very organized. Each event is labeled to identify and categorize victims. Cyberspace attackers commonly apply description to each victim – often hurling their victim to distinguish them from other attack victims. Victim categories make INTOLERANT interesting:

(TS//SI//REL) INTOLERANT's traffic is very organized. Each event is labeled to identify and categorize victims. Cyberspace attackers commonly apply description to each victim – often hurling their victim to distinguish them from other attack victims. Victim categories make INTOLERANT interesting:

(TS//SI//REL) INTOLERANT's traffic is very organized. Each event is labeled to identify and categorize victims. Cyberspace attackers commonly apply description to each victim – often hurling their victim to distinguish them from other attack victims. Victim categories make INTOLERANT interesting:

(TS//SI//REL) INTOLERANT's traffic is very organized. Each event is labeled to identify and categorize victims. Cyberspace attackers commonly apply description to each victim – often hurling their victim to distinguish them from other attack victims. Victim categories make INTOLERANT interesting:

(TS//SI//REL) INTOLERANT's traffic is very organized. Each event is labeled to identify and categorize victims. Cyberspace attackers commonly apply description to each victim – often hurling their victim to distinguish them from other attack victims. Victim categories make INTOLERANT interesting:

(TS//SI//REL) INTOLERANT's traffic is very organized. Each event is labeled to identify and categorize victims. Cyberspace attackers commonly apply description to each victim – often hurling their victim to distinguish them from other attack victims. Victim categories make INTOLERANT interesting:

(TS//SI//REL) INTOLERANT's traffic is very organized. Each event is labeled to identify and categorize victims. Cyberspace attackers commonly apply description to each victim – often hurling their victim to distinguish them from other attack victims. Victim categories make INTOLERANT interesting:

(TS//SI//REL) INTOLERANT's traffic is very organized. Each event is labeled to identify and categorize victims. Cyberspace attackers commonly apply description to each victim – often hurling their victim to distinguish them from other attack victims. Victim categories make INTOLERANT interesting: