(U) The Answer Is... Peer to Peer File Sharing

FROM: [redacted]
FAVA Pod (S3T1)
Run Date: 06/22/2005

(U) One corresponding question might be: **What technology is responsible for nearly two-thirds of all Internet traffic?** In fact, CacheLogic conducted a study (available at www.cachelogic.com) examining traffic from January 2004 through June 2004 which showed that over one-third of all Internet traffic is due to a single Peer to Peer (P2P) application: BitTorrent. Let's take a moment to ponder this. Think of all of the non-P2P traffic out on the net: web, email, voice over IP (voip), etc. It turns out that BitTorrent is responsible for more traffic than all of these -- combined!

(U) This is due in large part to the types of files typically shared using BitTorrent, namely movies and TV shows (many in High Definition!). What is even more amazing is that BitTorrent isn't even the most popular file-sharing application. The P2P-focused website Slyck.com publishes the number of users currently connected to many of the popular P2P networks, and the two file-sharing applications with the most users as of June 2005 are eDonkey and KaZaA with approximately 5 million and 2.5 million users respectively.

(U) If you're asking yourself what is a Peer to Peer application, you are not alone. Peer to Peer file-sharing is a relatively recent addition to Internet communication methods. In its most basic sense, P2P applications provide a way for two users to share files directly, without having to put the files on a central computer. The first P2P system to gain notoriety was Napster. That system became the target of the Recording Industry Association of America (RIAA), since many users were illegally sharing copyrighted music files. Many of the popular P2P networks today continue to be targeted by the RIAA for the same reason.

(S//SI) This is the backdrop against which the File-sharing Analysis and Vulnerability Assessment (FAVA) Pod began its research**. The first task was to find ways to efficiently identify P2P traffic to allow further processing. eDonkey has been a particular success story in this regard as we can identify most eDonkey traffic now by examining only a few bytes in a packet.

(S//SI) One question that naturally arises after identifying file-sharing traffic is whether or not there is anything of intelligence value in this traffic. By searching our collection databases, it is clear that many targets are using popular file sharing applications; but if they are merely sharing the latest release of their favorite pop star, this traffic is of dubious value (no offense to Britney Spears intended). Hence the next task was to decode the traffic of these P2P applications. As many of these applications, such as KaZaA for example, encrypt their traffic, we first had to decrypt the traffic before we could begin to parse the messages. **We have developed the capability to decrypt and decode both KaZaA and eDonkey traffic to determine which files are being shared, and what queries are being performed.**

(TS) The latest success on the KaZaA project was developing the ability to parse out the registry entries on a hard drive. Stored in the registry are e-mail addresses, country codes, user names, location of the downloaded files, and a list of recent searches -- encrypted of course.

(S) Using these tools, **we have discovered that our targets are using P2P systems to search for and share files which are at the very least somewhat surprising** -- not simply harmless music and movie files. With more widespread adoption, these tools will allow us to regularly assimilate data which previously had been passed over; giving us a more complete picture of our targets and their activities.

(S) The file-sharing applications the FAVA Pod has examined are: BitTorrent, DirectConnect, eDonkey, FastTrack (KaZaA), Freenet, Gnutella, Gnutella2, JoltID, MSN Messenger, Windows

Messenger, and Yahoo Briefcase. If you have a target using any of these applications or using some other application which might fall into the P2P category, please contact us -- we would be more than happy to help.

** Note:
(S) The Pod Research Program, S3T1, resides in the Technical Advocate Office. For more information, type "go pods" in your favorite browser.

"(U//FOUO) SIDtoday articles may not be republished or reposted outside NSANet without the consent of S0121 (DL sid_comms)."

NATIONAL
SECURITY
ARCHIVE

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu