

Cloudmark Research Report

Title: Kama Sutra (CME-24) Worm Outbreak Analysis

Date: 2/10/2006

Authors: Jason Harbert, Vipul Ved Prakash, Adam J. O'Donnell

The Kama Sutra worm first appeared on January 16, 2006 as an email message claiming to contain pornographic images and video. After infecting a host, the Kama Sutra worm first attempts to disable anti-virus software and then begins to propagate itself by e-mailing copies of itself to e-mail addresses found in infected host's address book. The virus also places copies of itself on open network shares. The virus incorporates automated update capabilities provided by the worm's author by connecting to a remote hostⁱ. The Kama Sutra worm was designed to begin destroying documents with the DOC, XLS, MDB, MDE, PPT, PPS, ZIP, RAR, PDF, PSD and DMP extension beginning on February 3, 2006. The document destruction component is not limited to the local machine, since the virus also attempts to delete any documents matching the above extension if they appear on shared folders locally attached to the system. The Kama Sutra worm is unusual in the e-mail virus space in that it actively destroys documents rather than attempting to backdoor the system for later use by the attacker. In an attempt to out-do one another, security companies rushed to assign a name to the virus without consulting one another, and as a result the virus goes by as many as a dozen other names. To avoid ambiguity, security researchers are also referring to the virus as CME-24ⁱⁱ.

Analysis:

Our first report of this virus came on Jan 16th, 4:42am PST. The virus became "spammy" at 5:08am PST, at which time it was being covered by the two fingerprinting algorithms in the Cloudmark Network Classifier – Ultra, an executable fingerprinting scheme, and Mishmash, a generalized binary fingerprinting scheme. Since Mishmash is present in all of our products, the virus was blocked for all of our customers as of this time. Analysis of fingerprint check log showed the virus spread to be minimal, but relatively prevalent within the first three days of its initial report. During its peak, on the 18th of January, the Kama Sutra virus appeared 4.5 times more often than it did on its first day. Afterwards, the virus died off and maintained a low status, until the 6th of February when it again spiked, this time appearing 8.7 times more often than it did on the day of its release. With a high degree of confidence, the research team is operating under the assumption that there is a new variant of Kama Sutra now present in the wild.

Further insight can be gathered by examining the virus relative to coverage by specific fingerprinting schemes. Sightings for the fingerprints created with Ultra were relatively low and highly variable due to its newness and the small number of clients that currently support it. However, Mishmash provided a far better metric for the virus's impact due to its wide availability across our product line. Overall, we saw 4072 checks against Mishmash fingerprints, and 643 checks against Ultra fingerprints.

It is noteworthy to mention that while Ultra covered all variants of the worm with a single fingerprint, Mishmash generated 2 fingerprints. This observation implies that the Ultra provides better multiplicity in the face of worm mutation. At this time, the research team is uncertain whether other anti-virus companies are capable of tracking the mutations or not.

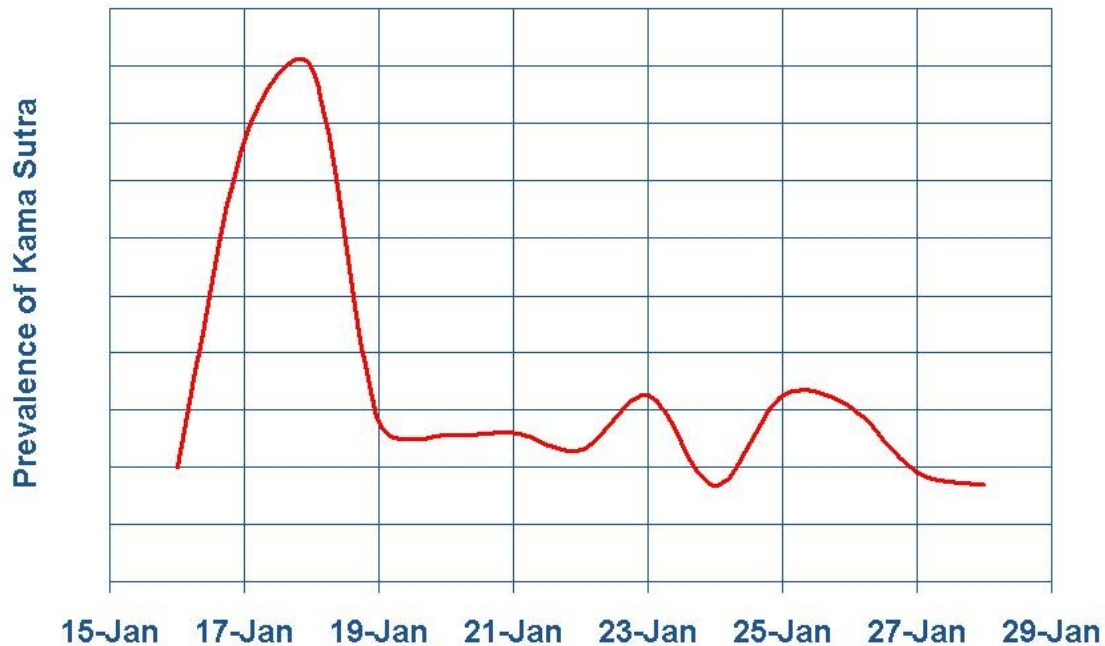


Figure 1. The initial peak covering January 16th through January 19th shows the propagation during the time in which anti-virus companies began blocking the virus. During the second peak, a new mutation of the virus formed which Ultra was able to successfully identify.

Summary:

The Kama Sutra virus gained large media attention due to its malicious intent and encoded destruction date, and also due to the name and expected content of its attachments. However, the virus spread was extremely low in our network of users and less than 2% of our entire network saw the virus. Other AV companies, such as McAfee, agree with this, saying that Kama Sutra infected a *maximum* of 15,000 machines inside the US, and gave the virus a low impact warning.

¹A summary of the infection and update process can be found at:

http://www.theregister.co.uk/2006/01/19/kama_sutra_worm/

²Details on the Common Malware Enumeration Scheme can be found on the MITRE website:

<http://cme.mitre.org/>