



PGPCoder Alert
infectionvectors.com
May 2005

Vector: User execution (mail, file share, etc. requires user to open)

Impact: High (encrypts files making them unreadable)

“Extortion-based attacks” in the realm of viruses has been described tremendously by Dr. Adam Young and Dr. Moti Yung in their pioneering work in “cryptovirology”.¹ The types of attacks they describe are extremely complex, as well as scary. The “cryptovirus” as a revenue-generator has not been documented extensively in the wild, making this alert somewhat unique and interesting.

PGPCoder is a Trojan that attempts to take the victim machine’s files hostage, forcing a user to pay for a “decoder” to be able to read documents that are encrypted. The file, which often appears as just encoder32.exe, can arrive via email, file share, or any other means; however, it currently has not been linked to any self-propagation mechanism.

The “extortion engine” encrypts files with the following extensions on any writeable media found connected to the local machine:

- ASC
- DB
- DB1
- DB2
- DBF
- DOC
- HTM
- HTML
- JPG
- PGP
- RAR
- RTF
- TXT
- XLS
- ZIP

In addition, it drops a text file into any directory which holds files that were encrypted. The text file, named “ATTENTION!!!.TXT” carries a simple message:

Some files are coded.
To buy decoder mail: n781567@yahoo.com
with subject: PGPcoder 000000000032

Previously, a version of this type of attack was documented with the following message²:

Some files are coded.
To buy decoder mail: asd67812@yahoo.com
with subject: PGPcoder 000000000022

The encryptor adds “PGPcoder” to the beginning of targeted files; ands makes them unreadable to users. Kaspersky Labs added a decryption routine to their product for a previous version of the encoder.

This piece of malware documents the number of files it successfully encrypts, via a Registry entry. The application also lists the directories/files found in a file it writes to the Windows TEMP directory.³ Once the malware has scanned/encrypted everything in its reach, it attempts to delete itself, presumably to hinder reverse engineering of its encryption routine.

References

1. “Cryptovirology: Extortion-Based Security Threats and Countermeasures”, Adam Young, Moti Young, Proceedings of the 1996 IEEE Symposium on Security and Privacy, 6-8 May 1996.

Adam Young and Moti Yung have completed very interesting research which is both extremely technical and very readable for virus researchers of all backgrounds. Details on their latest book, “Malicious Cryptography: Exposing Cryptovirology” (Wiley, 2004) can be found at:

http://www.amazon.com/exec/obidos/ASIN/0764549758/ref=pd_sxp_elt_11/102-0894264-2379328

2. In December of 2004, the same message, with different version and email addresses was listed on Viruslist’s weblog:

<http://www.viruslist.com/en/weblog?discuss=156387172>

The original entry for this thread shows other warnings and email addresses for decoding as well as mentioning the decryption routine built into the Kaspersky product:

<http://www.viruslist.com/en/weblog?discuss=156387172&return=1>

3. Trojan.Pgpocoder at Symantec’s site:

http://securityresponse.symantec.com/avcenter/venc/data/trojan_pgpocoder.html

TROJ_PGPCODER at Trend Micro’s site:

<http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ%5FPGPCODER%2EA>