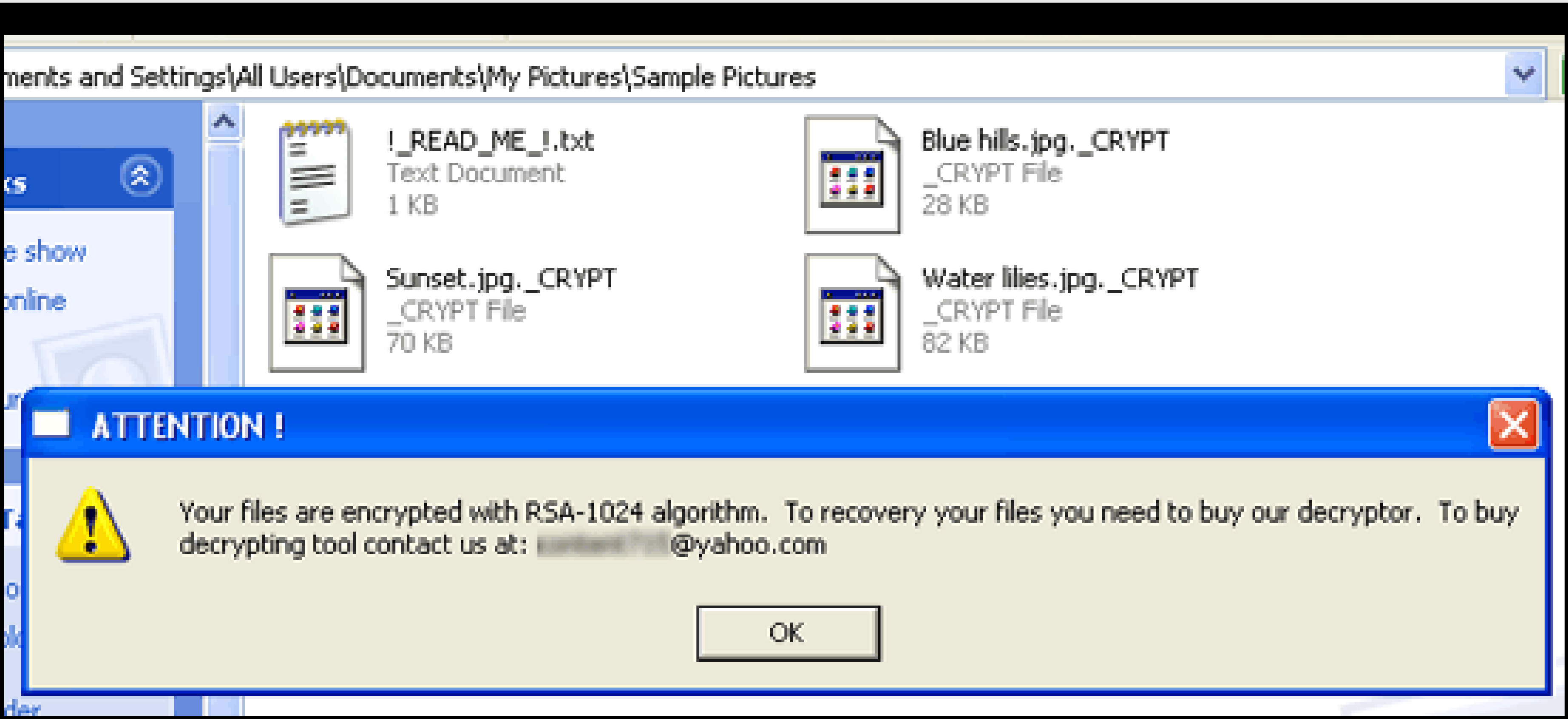
Cryptanalysis of the Gpcode.ak ransomware virus

Eran Tromer

MIT

The Gpcode.ak ransomware virus



ments and Settings\All Users\Documents\My Pictures\Sample Pictures

!_READ_ME_!.txt
Text Document
1 KB

Blue hills.jpg._CRYPT
_CRYPT File
28 KB

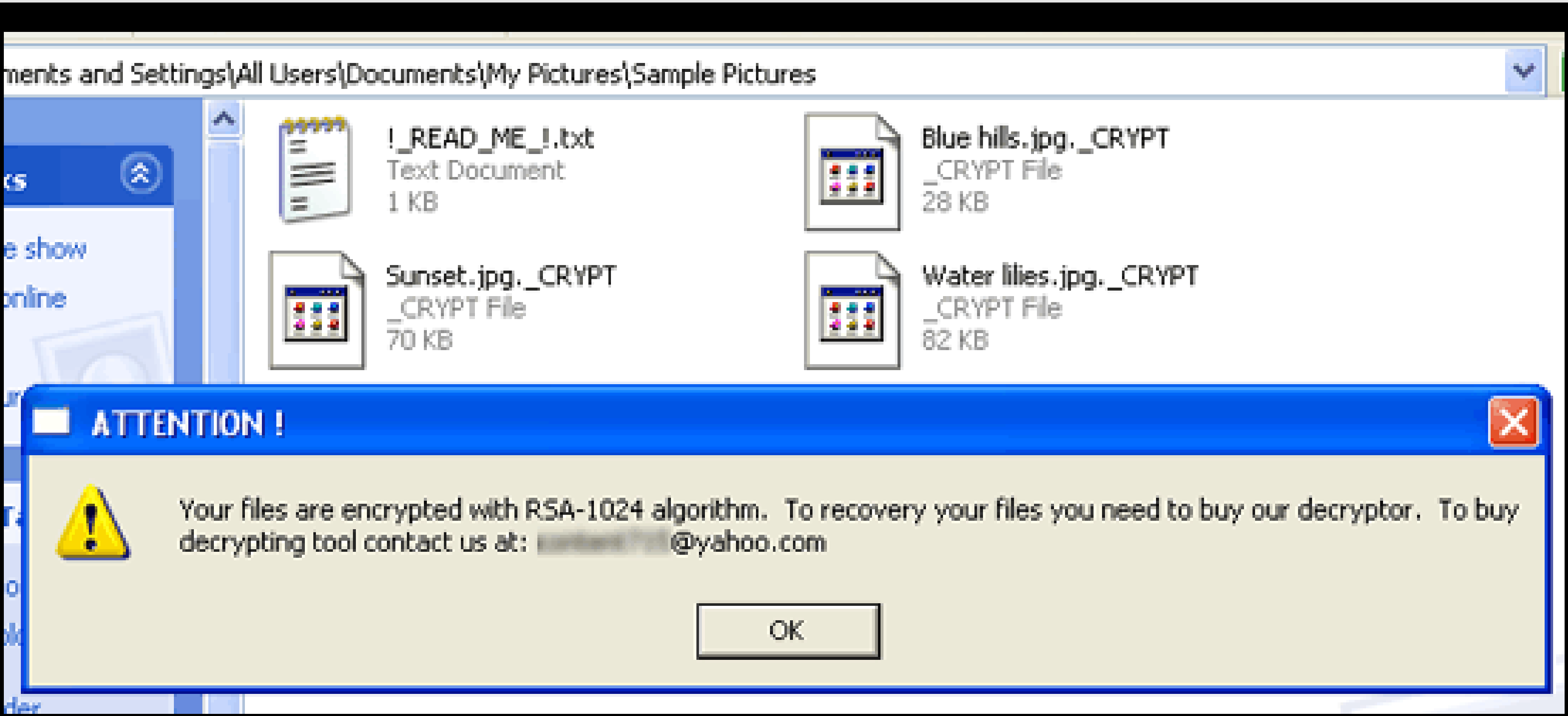
Sunset.jpg._CRYPT
_CRYPT File
70 KB

Water lilies.jpg._CRYPT
_CRYPT File
82 KB

ATTENTION !

Your files are encrypted with RSA-1024 algorithm. To recovery your files you need to buy our decryptor. To buy decrypting tool contact us at: [redacted]@yahoo.com

The Gpcode.ak ransomware virus



ments and Settings\All Users\Documents\My Pictures\Sample Pictures

!_READ_ME_!.txt
Text Document
1 KB

Blue hills.jpg._CRYPT
_CRYPT File
28 KB

Sunset.jpg._CRYPT
_CRYPT File
70 KB

Water lilies.jpg._CRYPT
_CRYPT File
82 KB

ATTENTION !

Your files are encrypted with RSA-1024 algorithm. To recovery your files you need to buy our decryptor. To buy decrypting tool contact us at: [redacted]@yahoo.com

OK

7z .abk .abd .acad .arh .arj .ace .arx .asm .bz .bz2 .bak .bcb .c .cc .cdb
cdw .cdr .cer .cgi .chm .cnt .cpp .css .csv .db .db1 .db2 .db3 .db4 .dba .dbb
dbc .dbd .dbe .dbf .dbt .dbm .dbo .dbq .dbt .dbx .Djvu .doc .dok .dpr .dwg .dxf
ebd .eml .eni .ert .fax .flb .frm .frt .frx .frg .gtd .gz .gzip .gfa .gfr .gfd
h .inc .igs .iges .jar .jad .Java .jpg .jpeg .Jfif .jpe .js .jsp .hpp .htm .html
key .kwm .Ldif .lst .lsp .lzh .lzw .ldr .man .mdb .mht .mmf .mns .mnb .mnu .mo
msb .msg .mxl .old .p12 .pak .pas .pdf .pem .pfx .php .php3 .php4 .pl .prf .pgp
prx .pst .pw .pwa .pwl .pwm .pm3 .pm4 .pm5 .pm6 .rar .rmr .rnd .rtf .Safe .sar
sig .sql .tar .tbb .tbk .tdf .tgz .tbb .txt .uue .vb .vcf .wab .xls .xml

Email

Next, you should send $100 to Liberty Reserve account U6890784 or E-Gold account 5431725 (www.e-gold.com) To buy E-currency you may use exchange service, see or any other. In the transfer description specify your e-mail. After receive your payment, we send decryptor to your e-mail. For check our guarantee you may send us one any encrypted file (with cipher key, specified in any !_READ_ME_!.txt file, being in the directorys with the encrypted files). We decrypt it and send to you originally decrypted file.

Best Regards, Daniel Robertson

Email 2

The price of decryptor is 200 USD. For payment you may use one of following variants: 1. Payment to E-Gold account 5437838 (www.e-gold.com). 2. Payment to Liberty Reserve account U6890784 (www.libertyreserve.com). 3. If you do not make one of this variants, contact us for decision it. For check our guarantee you may send us ONE any encrypted file. We decrypt it and send to you originally decrypted file. For any questions contact us via e-mail.

Best regards. Paul Dyke

(Russian criminals via a Chinese ISP)

Reverse-engineering Gpcode.ak

(based on a sample from Kaspersky Lab)

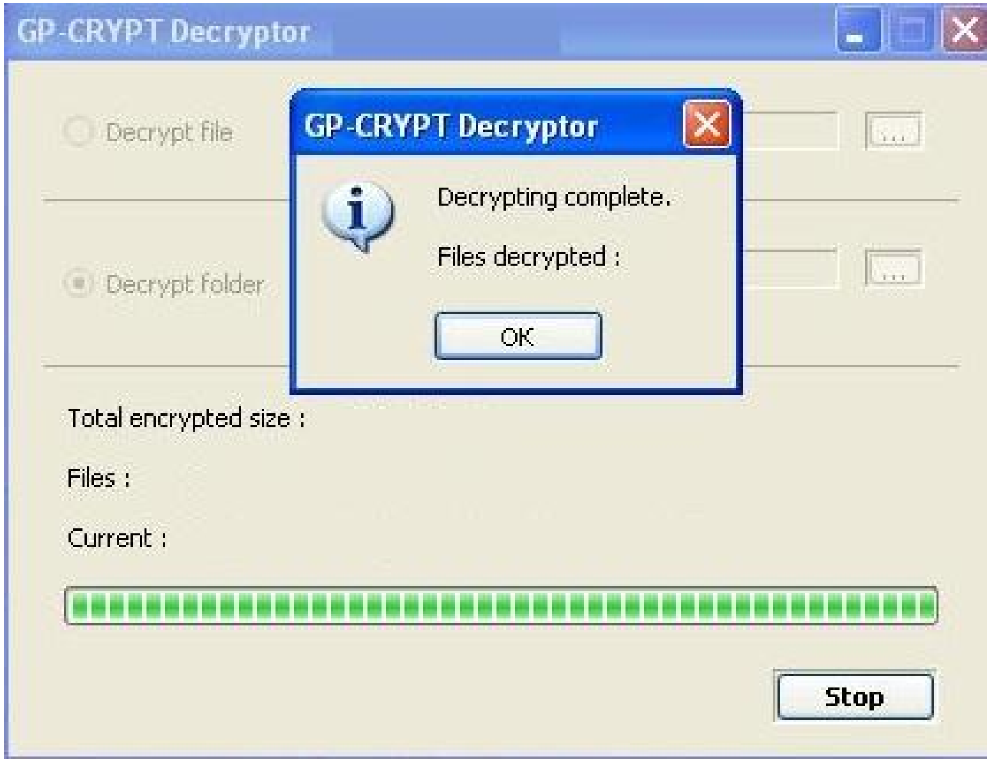
Virus payload

- Generate a random RC4 machine key K_{M}
- For every file f :
  - Generate random file nonce N_f
  - Derive an RC4 file key K_f from N_i and K_{M}
  - Encrypt the file using K_f and prepend N_f to the ciphertext
  - Delete original file
- Encrypt K_{M} under an embedded 1024-bit RSA public key and write it to **`_READ_ME_!.txt`**
- Forget K_{M}

All in 8030 bytes. Uses Windows CryptoAPI.

Decryption

- Victim sends `_READ_ME_!.txt` and $200 to "Daniel Robertson".
- "Daniel" decrypts the machine key K_{M} using his RSA private key and sends it to the victim, embedded in a "decryptor".
- Decryptor rederives the file keys.



GP-CRYPT Decryptor

Decrypting complete.

Files decrypted :

Total encrypted size :

Files :

Current :

Cryptanalysis

The Gpcode.ak 1024-bit RSA Factoring Challenge

- e=65537
- n_1=c0c21d693223d68fb573c5318982595799d2d295ed37da38be41ac8486ef900aee78b4729668fc920ee15fe0b587d1b61894d1ee15f5793c18e2d2c8cc64b0539e01d088e41e0eafd85055b6f55d232749ef48cfe6fe905011c197e4ac6498c0e60567819eab1471cfa4f2f4a27e3275b62d4d1bf0c79c66546782b81e93f85d$_{16}$

  or

  n_2=d6046ad6f2773df8dc98b4033a3205f21c44703da73d91631c6523fe735607247cc9a5e0f936ed75c75ac7ce5c6ef32fff996e94c01ed301289479d8d7d708b2c030fb79d225a7e0be2a64e5e46e8336e03e0f6ced482939fc571514b8d7280ab5f4045106b7a4b7fa6bd586c8d26dafb14b3de71ca521432d6538526f308afb$_{16}$

Cost of factoring a 1024-bit RSA modulus

- Exhaustive search
  - Don't be silly
- Number Field Sieve
  - TWIRL ($1M x year)
  - SHARK ($200M x year)

  + matrix step

  + NRE

  + energy

Key derivation weakness (there are others)

$$K_f \leftarrow \mathrm{RC4}_{K_\mathrm{M}}(N_f)$$

But RC4 is a stream cipher!

$$K_f \;=\; K'_\mathrm{M} \oplus N_f \quad \text{where } K'_\mathrm{M} = \overline{\mathrm{RC4}}(K_\mathrm{M})$$

Every file with known plaintext header gives:

$$N_f,\ \overline{\mathrm{RC4}}(K'_\mathrm{M} \oplus N_f)$$

Goal: recover the effective machine key K'_M .

Effective machine key recovery attack

- The setting is analogous to the [Fluhrer Mantin Shamir 2001] WEP attack, but the IV is XORed instead of prepended.
- Exploits (different) statistical biases in RC4:
  - [Roos 1995] [Maitra Paul 2007]
  - [Tews Weinmann Pyshkin 2007]
  - [Klein 2008] [Paul Rathi Maitra 2008]
- Combine biases optimally using Bayesian inference

partial

- Key recovery using ~10000 encrypted files (vs. ~25000 packets for WEP)

Conclusions

- Cryptanalysis saves the day!
  (if you have have a few thousand .jpg files on your disk)
- Open problem: UC-secure ransom scheme in the standard model