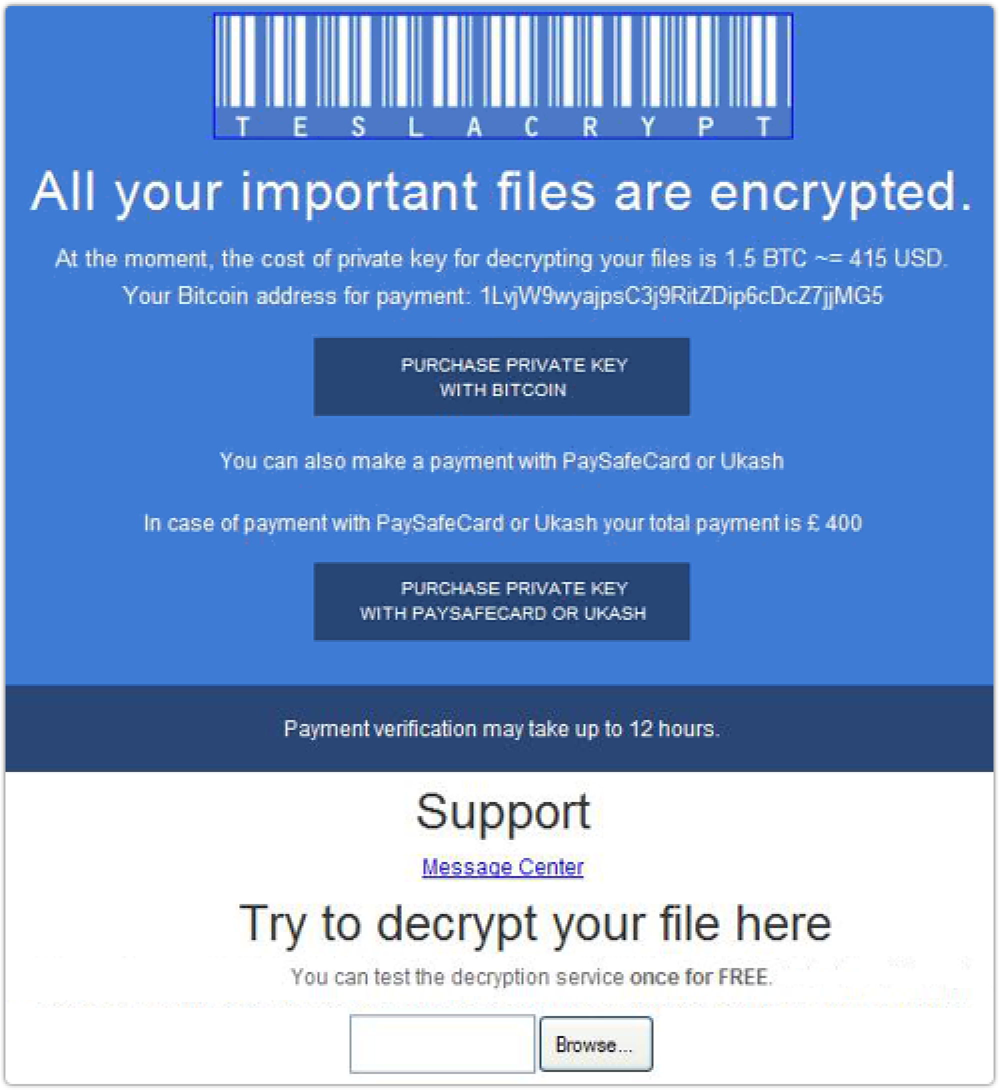
Security Now! #499 - 03-17-15

Q&A #208

This week on Security Now!

- A look at the new TeslaCrypt.
- Yahoo! SXSW splash about eliminating passwords.
- Comodo does it again… kinda.
- The InstantCryptor guys are getting warmer but are not there yet.
- 10 listener questions, comments and answers.



TESLACRYPT

All your important files are encrypted.

At the moment, the cost of private key for decrypting your files is 1.5 BTC ~= 415 USD.
Your Bitcoin address for payment: 1LvjW9wyajpsC3j9RitZDip6cDcZ7jjMG5

PURCHASE PRIVATE KEY WITH BITCOIN

You can also make a payment with PaySafeCard or Ukash

In case of payment with PaySafeCard or Ukash your total payment is £ 400

PURCHASE PRIVATE KEY WITH PAYSAFECARD OR UKASH

Payment verification may take up to 12 hours.

Support

Message Center

Try to decrypt your file here

You can test the decryption service once for FREE.

Security News

"TeslaCrypt" Ransomeware targets gamers

- To the lineup of CryptoLocker and CryptoWall, we add TeslaCrypt
- https://nakedsecurity.sophos.com/2015/03/16/teslacrypt-ransomware-attacks-gamers-all-your-files-are-belong-to-us/
- Does seek out photos, financial spreadsheets and Office documents.
- But ALSO seeks out files related to dozens of games, including saved games, configurations, maps and replays.
- TeslaCrypt targets some well-known games including Call of Duty, World of Warcraft, DayZ, Minecraft, Fallout and Diablo, as well as configuration files for Steam, the online gaming platform.
- TeslaCrypt also seeks out files related to tax returns, personal finance such as Intuit's Quicken software, and iTunes.
- TeslaCrypt can locate files on connected devices and drives and encrypt those too – USB drives, network file shares, cloud storage folders and other connected storage devices.
- Uses the proven approach pioneered by CryptoLocker:
    - Robust public key crypto that cannot be bypassed.
    - Time-limited payment.
    - Payment via bitcoin, "PaySafeCard, or Ukash.
    - Current ransom is: 1.5 btc, (about $420) or $600 via PaySafeCard or Ukash.
    - One "free" decryption to prove it's possible.

Yahoo! to eliminate passwords

- http://fortune.com/2015/03/16/yahoo-says-goodbye-to-passwords-is-it-a-good-idea/
- On Sunday at SXSW, Yahoo YHOO unveiled a new login procedure that does away with the need for remembering passwords. It's a welcome advance for digital security, but no panacea.
- Multi-factor authentication... or a different single-factor?
- The device can stand-in for the user.

Comodo does it again... kinda.

- http://arstechnica.com/security/2015/03/bogus-ssl-certificate-for-windows-live-could-allow-man-in-the-middle-hacks/
- https://technet.microsoft.com/en-us/library/security/3046310
- "COMODO RSA Domain Validation Secure Serve CA"
- How GRC used to get a simple domain validation cert: "Prove control of a domain."
    - Create a publicly accessible page specified by the registrar.
    - Respond to an eMail at one of several administrative accounts:
      Comodo: 'admin', 'administrator', 'postmaster', 'hostmaster' or 'webmaster'
- ARS/Dan Goodin: <quote> The ease in obtaining such certificates, and the difficulty in killing them off once they're issued, are potent reminders of the continued insecurity of one of the Internet's most important security mechanisms.
-

- An automatic updater of revoked certificates is available for Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2:
    - http://support.microsoft.com/en-us/kb/2677070

"InstantCryptor" - getting better, but not yet quite right

- Tweet: CloudRail @CloudRail
  @SGgrc Thanks for your feedback about #InstantCryptor. We've updated it according to your advice to make it even more secure. Any feedback?

- Email:
  Subject: Feedback on instantcryptor.com
  Location: Mannheim, Germany

  Hello Steve,

  One of your listeners, who calls himself "Advait from India", has made us aware that you've discussed instantcryptor.com in your podcast. I'm the main developer behind this product and was eager to learn about your opinion. In fact we've modified the encryption procedure such that now the plaintext plus a hash value of that very plaintext is input for AES-CBC encryption, which allows us to check upon decryption if the password used was correct and if the message has been modified. I'd be happy to get feedback from your side and could provide you with more details. Feel free to contact me under the mentioned email address.

  Regards, Florian

- Encrypt({PlainText}+{SHA256{Plaintext})
- Goals:
    - Detect wrong password
    - Detect ANY modification
- This DOES detect wrong password, but doesn't robustly detect modification.
- The HASH is still inside of the encryption, and it is not keyed with a secret key.

- Taylor Hornby (aka FireXware) -- defuse.ca:
  The quick answer is that it's well-known how to forge messages under this scheme. The attack is pretty neat. It's explained in the second part of this answer:

  https://crypto.stackexchange.com/a/16431

  It's pretty bad because the requirements of the attacker are strictly less than chosen-plaintext. For example, if Alice has uploaded mspaint.exe file and Dropbox can get Alice to upload a file containing evil.exe anywhere inside it (aligned on a block boundary), then Dropbox can replace mspaint.exe with evil.exe.

  The more complete answer is that today the burden of being called "secure" is to have been proven secure in an indistinguishability/non-malleability model:

https://en.wikipedia.org/wiki/Ciphertext_indistinguishability

The dominant attitude today is that, instead of finding and fixing individual problems, we just outright refuse to accept anything that isn't proven IND-CCA2-secure (INDistinguishability under adaptive Chosen Ciphertext Attack). That's the important lesson: You can't iterate on crypto design by fixing problems that come up, you have to start with something (proven) secure, and we *have* things that are proven secure (encrypt-then-HMAC).

(The Telegram messenger is another example of ignoring this lesson)

- (Taylor consults. He really enjoys performing crypto auditing -- use him!!)

Miscellany:

The LHC is coming back up.

- Operating power:
    - Before: 8 TeV (trillion electron volts)
    - Now: 13 TeV

  They WANT to find something off to challenge they current model.

SpinRite:

Brandon <anon@grc.com>
Location: Wisconsin
Subject: Spinrite GPT/EFI/UEFI?
Date: 02 Mar 2015 19:48:56

I'm a long time listener, and user of your products (it all started for me with ShieldsUP!), and I've been wondering about your future ideas for SpinRite.

I know that you're re-writing it for much faster speeds and all sorts of wonderful features we’ve heard about, but I don't believe anyone's brought up the compatibility side of things: Are you planning on updating SpinRite to work with GPT formatted drives, drives that SpinRite 6 doesn't agree with because they are "MBR Followed by EFI", and are you planning on adding UEFI boot support?