TRUSTED CRYPTOGRAPHIC MODULES, MALWARE AND ENCRYPTION

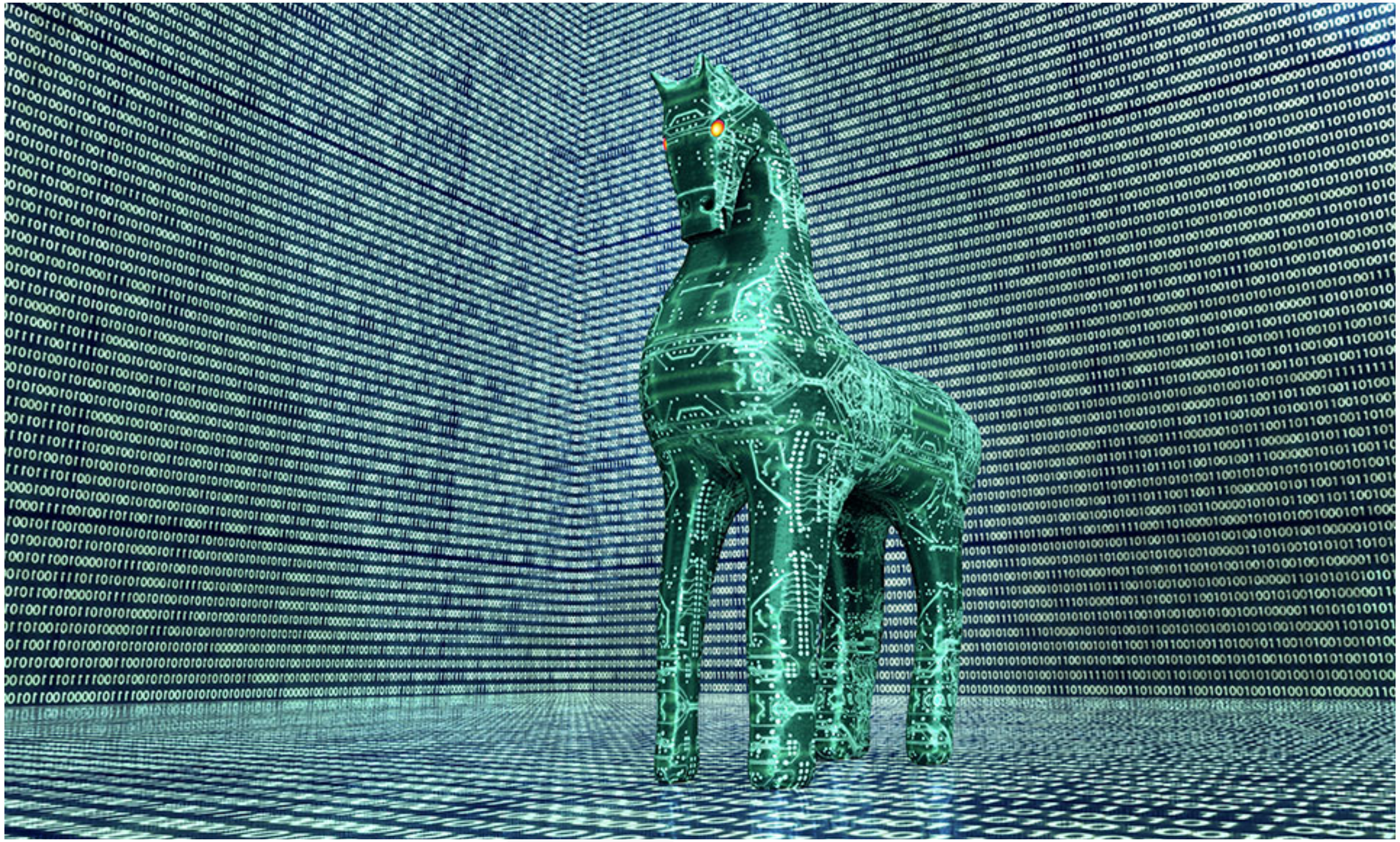
STEVE SCHMALZ, FIELD CTO, RSA PUBLIC SECTOR

MALWARE ENCRYPTION

TALENTED AMATEURS…

MALWARE FIRST USED ENCRYPTION TO HIDE…

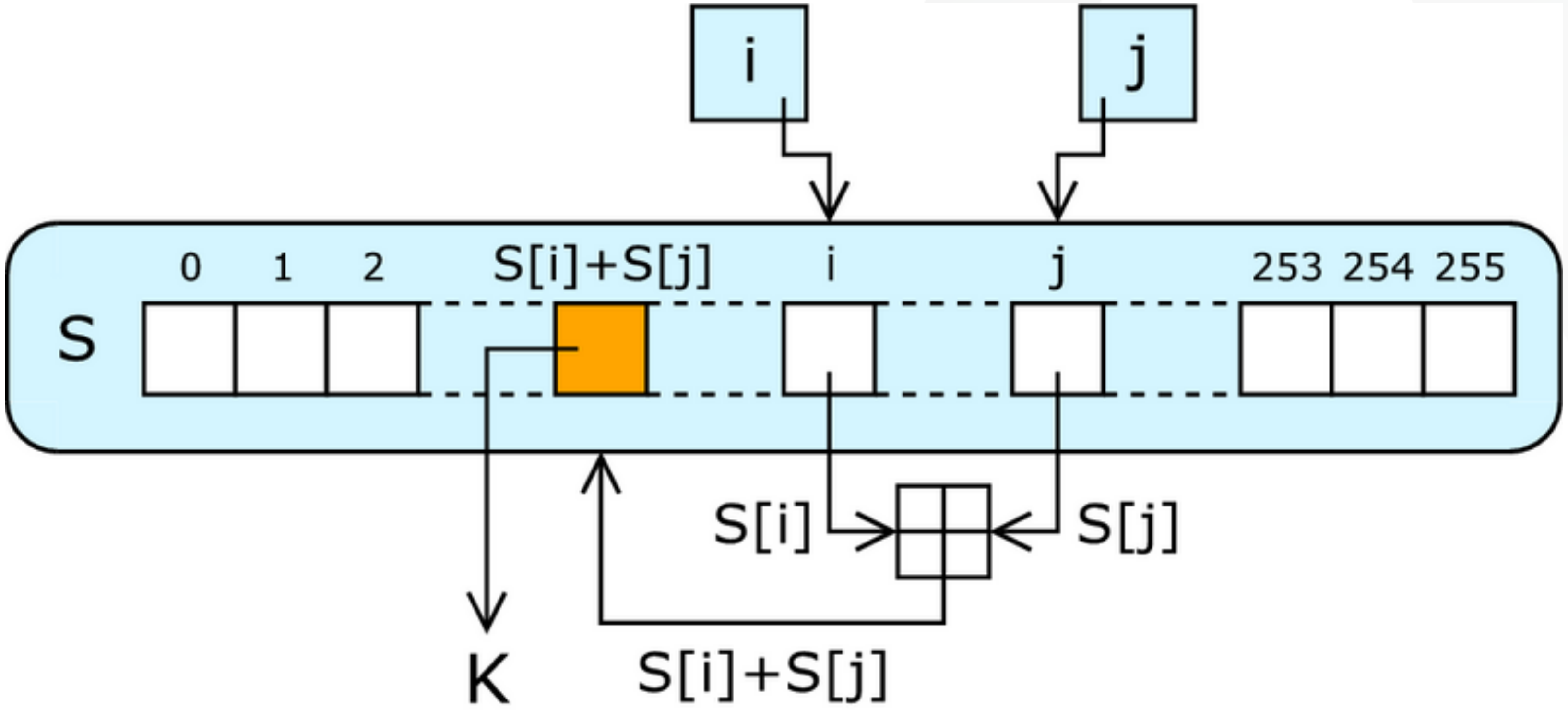
MALWARE OBFUSCATION



RSA

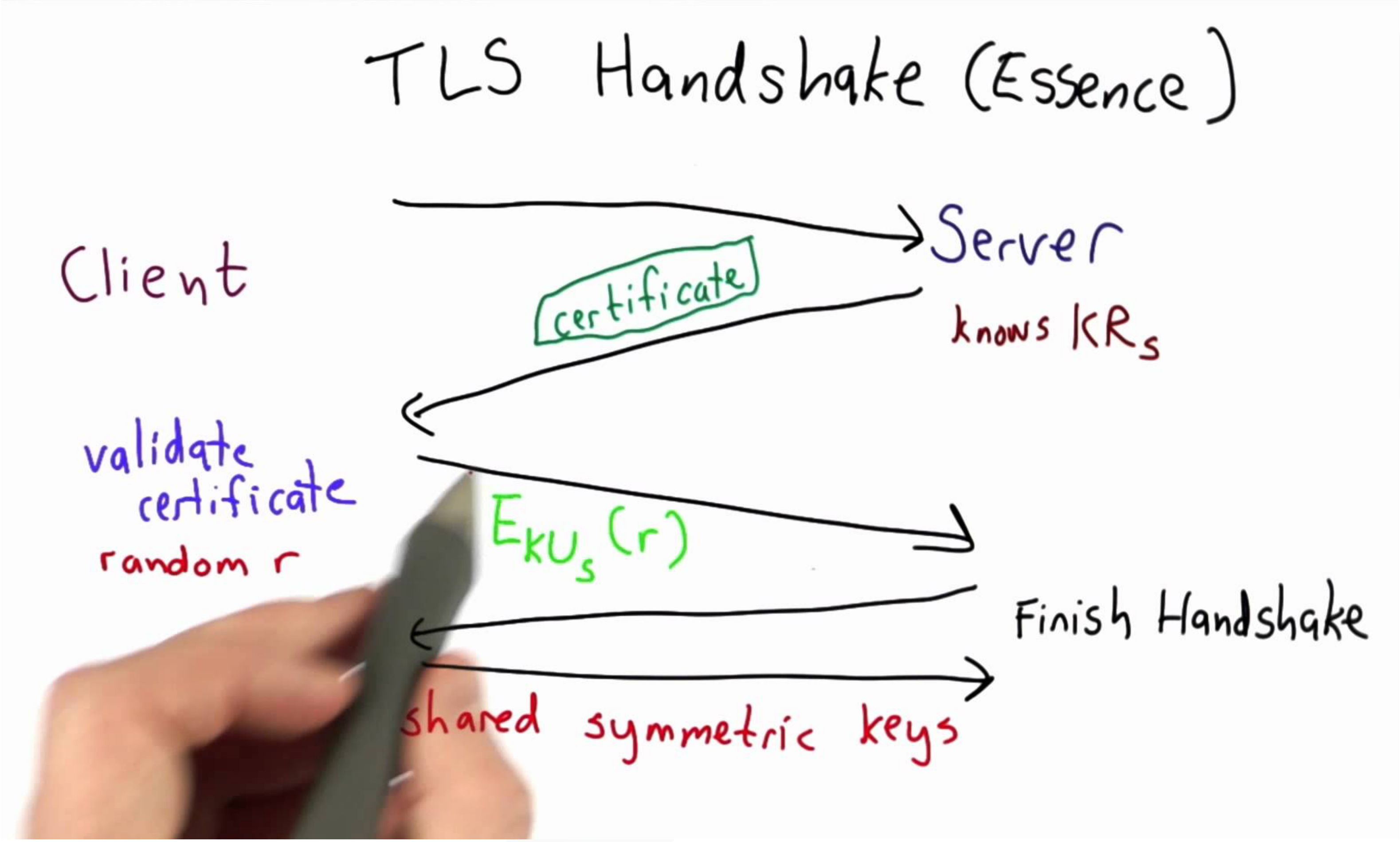
THEN SIMPLE ENCRYPTION EMBEDDED IN THE MALWARE CODE TO PROTECT COMMAND CONTROL LINKS.

RC4 WAS FIRST USED IN SPYEYE AND ZEUS ALONG WITH MULTIPLE XORS IN 2007...



MOST RECENTLY MALWARE IS LEVERAGING SSL USING LIBRARIES ON THE HOST.

FORTUNATELY, SSL/TLS HAS META DATA



HOW DO WE FIND MALWARE THAT USES ENCRYPTION?

THE CHALLENGE FOR THE PROFFESIONALS...

MONITORING NETWORKS, LOGS AND ENDPOINTS

ENCRYPTION HIDES MALWARE IN EACH CASE

Endpoints

- Encryption prevents signature based discovery
- Although behavior based methods still work

Network

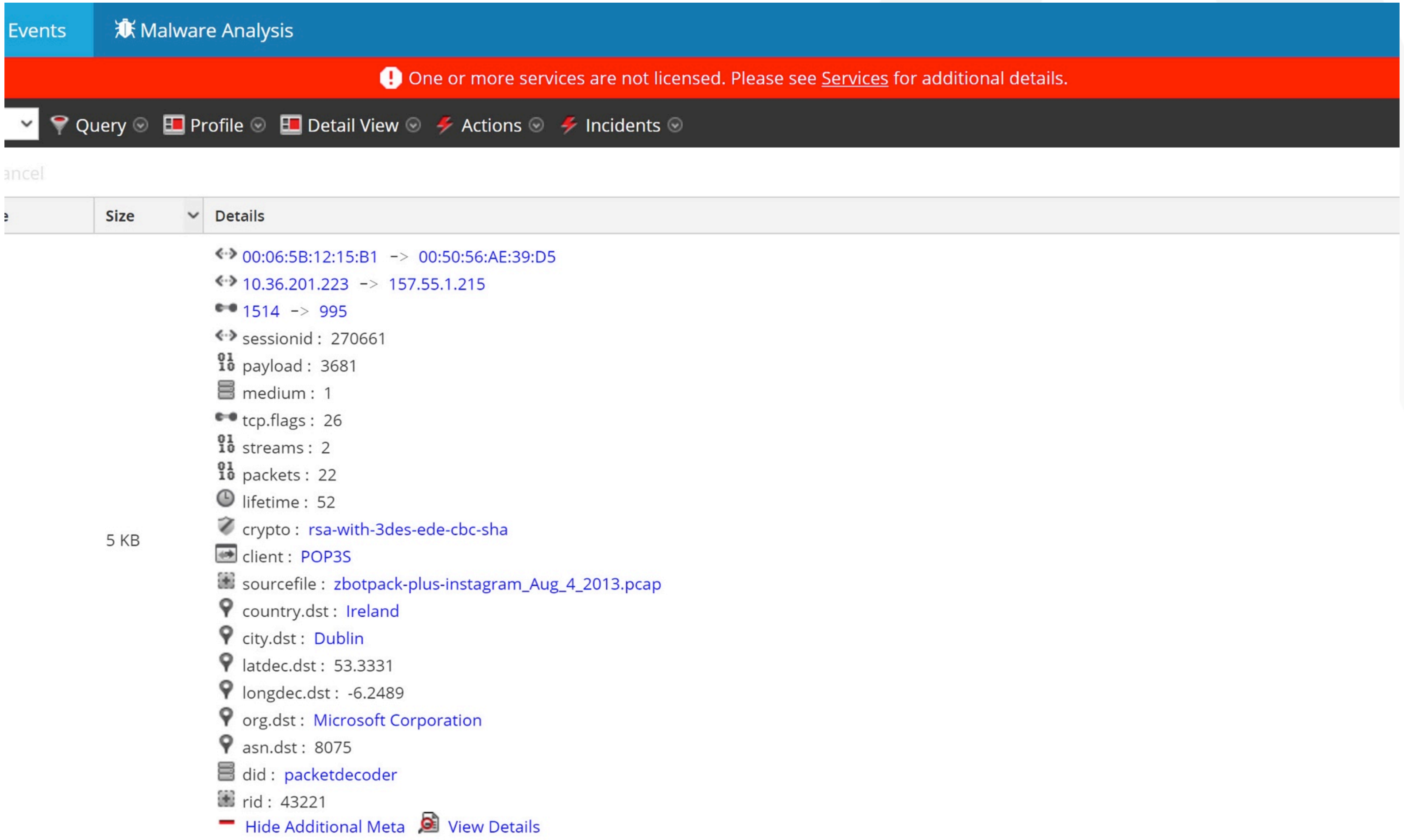
- Use of encryption and SSL hides CC coms
- Although traffic characteristics might identify suspicious traffic
- Still, CC traffic usually encrypted twice…

Logs

- ?

SSL METADATA IS AVAILABLE

EXAMPLE



One or more services are not licensed. Please see Services for additional details.

5 KB

00:06:5B:12:15:B1 -> 00:50:56:AE:39:D5
10.36.201.223 -> 157.55.1.215
1514 -> 995
sessionid : 270661
payload : 3681
medium : 1
tcp.flags : 26
streams : 2
packets : 22
lifetime : 52
crypto : rsa-with-3des-ede-cbc-sha
client : POP3S
sourcefile : zbotpack-plus-instagram_Aug_4_2013.pcap
country.dst : Ireland
city.dst : Dublin
latdec.dst : 53.3331
longdec.dst : -6.2489
org.dst : Microsoft Corporation
asn.dst : 8075
did : packetdecoder
rid : 43221

A GREAT REFERENCE ON THE USE OF TLS BY MALWARE

Deciphering Malware's use of TLS (without Decryption)

Blake Anderson, Subharthi Paul, and David McGrew (Cisco)

https://arxiv.org/pdf/1607.01639.pdf

From papers abstract:

"… TLS also introduces a complex set of observable data features that allow many inferences to be made about both the client and the server. We show that these features can be used to detect and understand malware communication, while at the same time preserving the privacy of benign uses of encryption."

TIME TO BE PROACTIVE

A CHALLENGE FOR THE STANDARDS COMMUNITY…

TLS IS NOT A "STATIC" PROTOCOL

CREATE MORE METADATA!!!

Multiple versions of SSL/TLS have been developed over the years…

Standardize a field that could be used by cryptographic modules to insert "trusted cryptographic source" tags.

- Challenges
  - Time
  - Privacy protection
  - Industry and CMVP support

ROOTS OF TRUST…

USE FIPS 140 VALIDATED CRYPTOGRAPHIC MODULES TO PRODUCE "TRUSTED CRYPTOGRAPHIC SOURCE" TAGS?

FIPS 140-2 Inside

QUESTIONS, FEEDBACKS, RANTS …

STEVE SCHMALZ, FIELD CTO, RSA PUBLIC SECTOR
STEVE.SCHMALZ@RSA.COM