

BSidesROC 2014 Crypto Puzzle

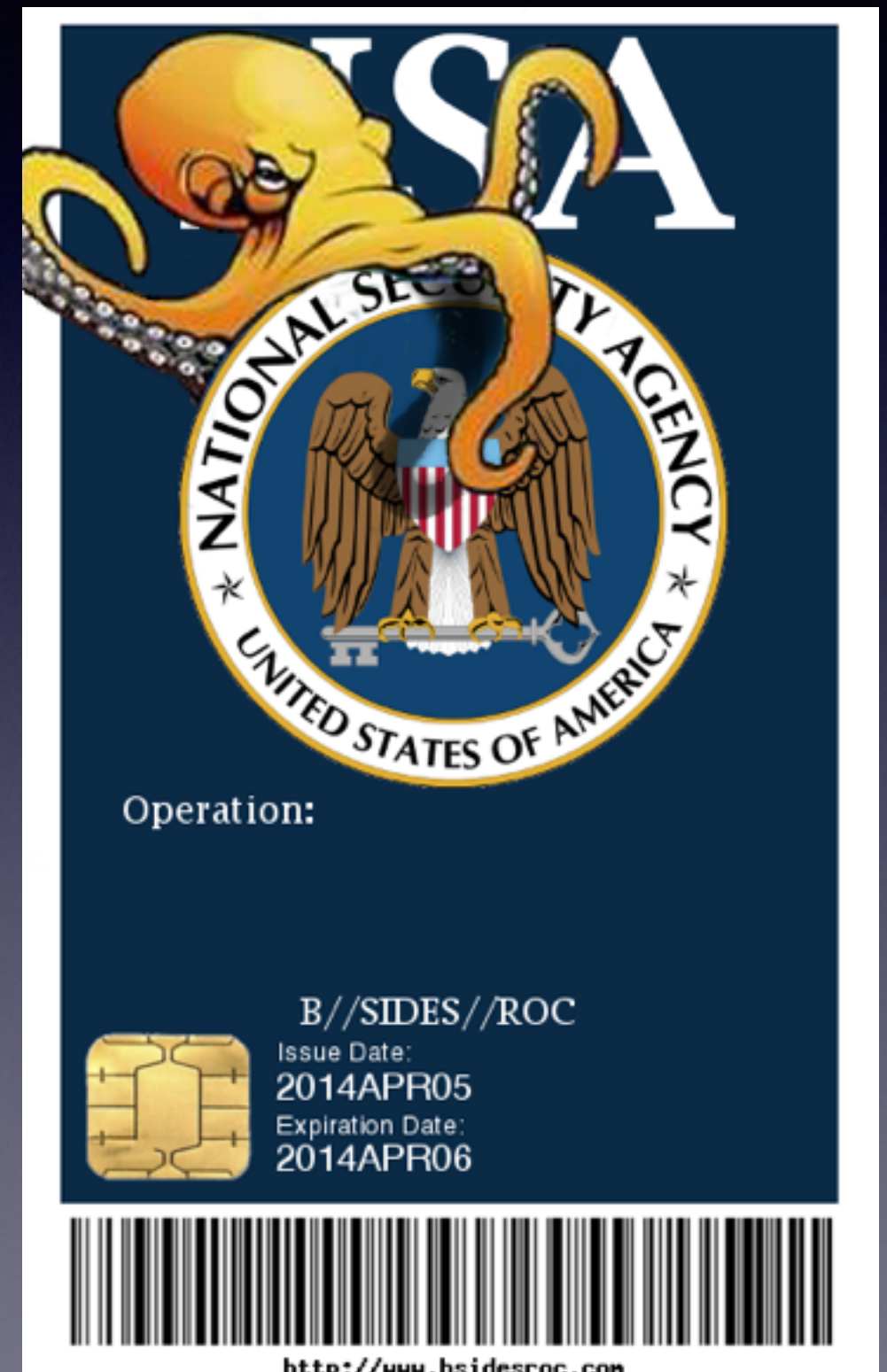
Created by Darth Null

(Sorry I can't be there in person....one con a month is my limit)



Welcome to the puzzle

- Changed things up a bit
- Half scavenger hunt
- Half crypto puzzle
- Shortcut for the final stage



Your mission...



TOP SECRET // NOFORN/ORCON

Date: April 5, 2014

Subject: (TS//NF) Suspected dead drops in vicinity of Rochester, NY

(TS//NF) Chris is a spy. Yuri is his handler. Neither of them is very smart. They're communicating via Dead Drops, and could really learn a thing or two about tradecraft. In fact, they're so dumb that they leave their messages behind after reading them, a fact which we in the Counterintelligence branch can exploit.

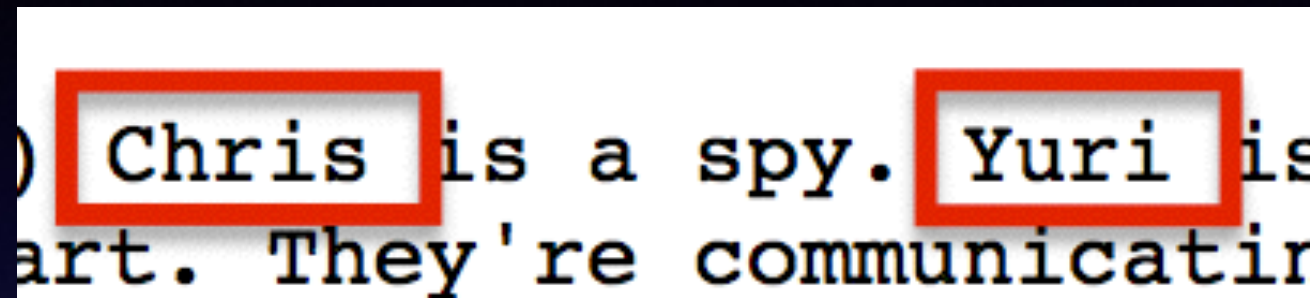
(TS//NF) Though Yuri and Chris are only slightly more intelligent than Boris Badanov and Maxwell Smart (combined!), we still remain very concerned about what they might be plotting. Therefore, we are assigning every possible agent to the task of recovering and reading their messages.

(TS//NF/OC) However, even we aren't great at cryptography, so we require that agents leave the messages where they are found, in case the messages' location may provide clues to subsequent agents as to the ciphers or keys in use. It's also possible that the subjects are so stupid as to reveal keys and/or methods within their actual messages. Determining whether this has occurred, and how to exploit such weaknesses, is left as an exercise for the agents in the field.

Your mission...

- Set out some ground rules
 - (don't screw with the hidden puzzle pieces!)
- Gave a few hints
- Told you how to deliver the winning solution

Inside jokes



) Chris is a spy. Yuri is
art. They're communicating

- Chris:
 - Jokingly refers to Christopher Boyce (The Falcon)
- Yuri:
 - Yuri Andropov (Former KGB head and Soviet Union leader)

Not making this up

- Major Hacker = Major Hacker

Agents who complete the mi
ults to @BSidesROC as quick

Classified by: **Maj C. Hacker**
son: 1.4(c, g)

*DEPARTMENT OF DEFENSE (DOD)
INFORMATION OPERATIONS CONDITION
(INFOCON) SYSTEM PROCEDURES*

ICATION IS MANDATORY

StratWeb Publications page.

Certified by: J010 **(Maj Cort O. Hacker)**

Pages: 35

- More throughout, some subtle, some not
- No importance other than just being lulzy

Dead Drops!

- Mixing in a scavenger hunt / geocaching vibe
- Suggested ideas for drop styles & markings
- But blame Jason and Mark for actual hides
- (Hope they were fun!)

Stage 1: Introduction

- Yuri and Chris meet.
- Caesar Cipher (ROT-4, for BSidesROC 4)

```
1Y  Lipps. Tpiewi xs viwtsrh amxl qiwweki  
hixempmrk csyv eggww. - CYVM
```

```
1C  Jmvwx, ythexi csyv gmtliv - ex piwx  
gsqi mrxs xli wmbxiirxl girxyvc. Xlir ai ger  
xepo efsyx JVIRGL LSZIVGVEJX, sv alexiziv  
csy pmoi. - GLVMW
```


Stage 1: Introduction

1Y Hello. Please to respond with message detailing your access. - YURI

1C First, update your cipher - at least come into the sixteenth century. Then we can talk about FRENCH HOVERCRAFT, or whatever you like. - CHRIS

- Next cipher hints: 16th Century & French = Vigènere
- Key: HOVERCRAFT (NOT full of eels)

Stage 2: Tasking

2Y ZDVWZ DFNTP DSVVV UVCZK LWVQE GVDTY
KOOEJ QESZI LFXEE PFNX

2C AVZFZ IXEXM JOIRF PZKSH DCALL TCSUN
TDFME UFVJK HADPV VYEDK LWIHV NRWFK LWNXY
CKSZI LFZRF WXHUL AIMRJ QLTHB HQVRT TRCPM
OWNGZ RYEWT WDVVV PKLDB AGPWV FFNFL JIGTK
WIENG AVZMI NLNHA YCJQK JVYON ZHYSE VGLFR
MODV

Stage 2: Tasking

2Y Spasibo. Now we are secure. I am need of datas on super cannons.

2C The biggest cannon I know of hurls pumpkins over a mile. They're in Delaware. Is that super enough? (PS - turns out CIA can crack this cipher -- apparently it's used on a sculpture in their lunchroom. They just don't Play Fair.

- Next cipher: Playfair.
- Key = KRYPTOS (name of sculpture at Langley)

Stage 3: Further Detail

3Y EFMSY FSLLO LGSYI AQPBM OMMLR DIAQP
BMGGI GYSHH QKCRL VMNHS BMCQL EHSBM IBMGL
KLVSY HFCBE BADYB LQPZ

3C CBEBA DYBLQ KQHYD FCBEB OBQGB MEIHR
DFBOS HVLYS KQBIO VSLBR HSMDP KPTDS GABFK
PRGAD YBLQY QFSMX DQVLV FCEDK IEAVQ KHQOQ
TGLSA BFBLQ ASAAA MSKCQ HVNDW CEB

Stage 3: Further Detail

3Y Delaware - is near Montana? I like Montana. And rabbits. Tell me, can these cannon fire large bags of paint?

3C Bags of paint? If the bags can handle the acceleration, sure. Specify type of bag, type of paint. Meanwhile, we should switch ciphers again - sorry for the ZigZags.

- Yuri would like to live in Montana.
- He also wants to hurl large bags of paint.
- Chris changes ciphers AGAIN

Stage 4: Arrange Delivery

```
4Y P*h*tanlmIe**rIsE**e*uo*astte.FaeotA  
gcaba*sIm-adbeiSTutL*oe.Is*rnort*ES.iio*  
*kir*c**e*sur.*b?*mlypoOIm*Bctft*oceoY*p  
iHUSn**epnr*t*Lslsssiepo*S*o*urPO*DUrpfr  
coihw*cysTXRtbieooe*nrPts*NOyohp.r*O
```

- Railfence cipher
 - Write plaintext in zig-zags
 - Read ciphertext across top
 - P*h*.... astte.F... iio**ki...

P	*	h	*			
a	s	t	t	e	.	F
i	i	o	*	*	k	
n	*	*	e	p	n	
t	b	i				

Stage 4: Arrange Delivery

```
4Y  Paint is to be the pink. Fire rate to
coat Los Angeles class submarine. Is
problem? PS - am told by superior POSITION
must DOUBLE crypto effort. I choose cipher
now. Your crypto is THE SUXORS.
```

- Yuri wants to paint submarines pink.
- Also sick of Chris' incompetent cipher tradecraft
- Next cipher: DOUBLE transPOSITION, keys THE & SUXORS

Stage 4: Request Key

```
4C  ATIOISHEHTUYPEPNGMENETRACYOLISDBREES  
VOEUWTPSVCIHENYRHTATFLTANKOEUHNEYMOHEIHC  
ETDTIIUONAOHSOSHCLXRXCDFRGIEELO
```

- Chris responds by asking for a hexadecimal key
- Challenges Yuri to a cipher game of his own

```
4C  Have photographed cannon. Send sixteen-  
byte key via the cipher of your choice,  
don't tell me which. I'll figure it out.  
"The suxors" my ass.
```

Stage 5: Yuri's Key

```
5Y Greetings, comrade! Is great day for
breakfast! Please to tell is bacon
considered extravagant? I would very much
like to be having a big breakfast with
bacon. Send link to good restaurant?
```

- Not a cipher, but steganography
- Length of each word is a single nibble
- Greetings = 9, comrade = 7 => 0x97

```
9725 3396 2425 ab15 4442 2613 9454 424a
```


Stage 5: Link to Image

```
5C: I HIGHLY REcOmMEND THE wAFFLE hOUSE fOR  
BREakFaST. BuT I WOUlD noT eAt The DAIlY  
SPeciaL, AS It IS mAde fROM laST NIghT'S  
leTtoVeRS.
```

- Uses a “Baconian” code (more stego):
 - Letter case represents binary bits, 5-bit words

```
bsides roc com dhrtzngpw bmp
```

Image of Super Cannon?

- Encrypted with Yuri's key:
 - 9725 3396 2425 ab15 4442 2613 9454 424a
 - 16 byte key implies AES-128
- No initialization vector provided
 - Electronic Code Book mode (ECB)
- Easily decrypted with openssl

Decrypted!

TELL US

ROC ROX

FTW

Shortcut!

- But wait! AES-128-ECB. Bad choice.
- Identical blocks produce identical ciphertext
- Very very bad for a bitmap image

Verify picture size

- Good guess: 1024 x 768 x 32-bit color
- $1024 * 768 * 4 = 3145728$ bytes
- Bitmap (.bmp) files have a 54 byte header
- $3145728 + 54 = 3145782$ bytes
- Pad up to next 16-byte block: 3145792 bytes

```
$ ls -l dhrtzngpw.bmp  
-rw-r--r--@ 1 dschuetz  staff 3145792 Apr  3 09:52 dhrtzngpw.bmp
```

Replace the Header

- Remove 1st 54 bytes of the ciphertext
- Replace with valid 1024x768x4 .bmp header
- Open in image viewer
- Win!

Who needs a key?



Thanks for Playing!