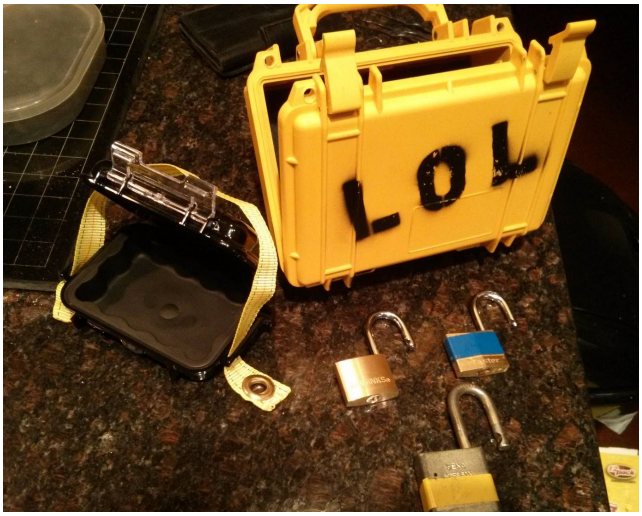
rogue signal

MISSION REPORT

Mission Name:
LOL Bitcoin Party Access Challenge
Location:
Las Vegas, Nevada
Challenges:
Various information security, hacking, and cryptography challenges.
Audience:
Skilled hackers and information security professionals attending the BlackHat and DEFCON conferences
Game Type:
Custom, Competitive, Very Difficult, Puzzle, Access Challenge

For a private party in 2013, instead of a standard invitation, we issued a multi-phase access challenge with multiple paths to success. This game was built to test various types of hacking and information security related skills while rejecting those without. Puzzle information was given to the player in a number of ways, including through images, encoded in hexadecimal data, translated from old languages, hidden on social media accounts and IRC channels connected to the convention.

Phase 1 required the players to convert hexadecimal data into a cipher and then translate that into the Twitter hashtag #LOLBitcoin. Following the attached Twitter account led the players to Phase 2.



Phase 2 included multiple ways to move forward, each with their own set of challenges within that category including reverse engineering, lockpicking, cracking passwords, network analysis, and solving ciphers. Players were encouraged to attempt different ways and to choose the one that was the best for them. Solving any of these got you an email address where you could begin Phase 3.

The email address in Phase 3 forced players to email using encryption in order to teach and encourage people to email using best information security practices. That email address would respond with a unique Bitcoin address, requiring the players to pay less than a penny in BTC (but would now be over $5 in late 2017 USD conversion rates!)

Phase 4 required the players first to BASE64 data and then combine it with the answer to a riddle. This gave a GPS location feed for a non-player character who went by The Whyte Rabbit. Using the GPS location the player had to physically find The Whyte Rabbit at DEFCON or Black Hat.
Once a contestant had found them, they were required to give their unique passphrase from the challenge and confirm the email address they used in Phase 3. If both were correct, they received a badge to the party!

If you have a background in information security, you might enjoy the full solution walkthrough that follows!

Full Solution to LOL Bitcoin 2013 Access Challenge

Phase 1 – Path 1: IRC/SILC

We had created channels on multiple IRC and SILC servers, each designed to point you in the correct direction. FreeNode and EFNet IRC networks had #LOLBitcoin channels with channel topics of "You're using the wrong technology…", indicating that you should either be looking at SILC (or at Twitter). The SILCNet SILC network had a #LOLBitcoin channel with a topic of "You're on the wrong network…", indicating that you were on the wrong SILC network. The CompSec SILC network had a #LOLBitcoin channel with the topic "Welcome to the Official LOL Bitcoin Party Channel! SysOp: @BitcoinTao".
"@BitcoinTao" could be interpreted as a chat user with ops, of which there was none in the channel, or as a Twitter account, which was the correct interpretation.
Phase 4 primarily involved tracking and hunting down the Whyte Rabbit. The Rabbit was not necessarily always the same person, but was the person currently carrying the Rabbit Bag which contained badges for the party, lanyards, some swag, and the Rabbit Phone. The Rabbit Phone was GPS tracked and configured with Twitter, Foursquare, and Instagram social media accounts.
If you haven't figured out the solution to the riddle above yet, it's "prints". By plugging in "prints" in place of the question marks in the URL, the location of the Rabbit was uncovered as the URL pointed to a page that was constantly updated with the GPS coordinates of the Rabbit Phone, which could be used to fairly accurately track down the Rabbit, assuming the Rabbit was not in a casino or other large building where cell phone reception and GPS tracking becomes unreliable.

Phase 1 – Path 2: Twitter Mining

The other path taken when presented with "#LOLBitcoin" is to interpret it as a social media hash tag. By digging through search results on Twitter for the hash tag "#LOLBitcoin", a single post using the hash tag from Twitter account @BitcoinTao could be found.

Phase 2: Choose Your Path

Finding the @BitcoinTao account on Twitter is the beginning of Phase 2 and was clearly indicated as such in the account's meta data. @BitcoinTao had posted on July 26th the message:
Be patient, and the way shall open itself to you… 癸巳年六月廿二 【癸巳年己未月丙申日庚寅時】 #LOLBitcoin
This message, using the "#LOLBitcoin" hash tag, allowed the account to be found from the final clue from Phase 1, but did not post the beginning clues to Phase 2 challenges until the early morning of July 29th, the Monday before BlackHat, as some of the challenges needed to be set up on-location or certain people involved needed to be in Las Vegas and available to provide their challenges. The Chinese characters in the tweet are old Mandarin and indicate the date and time of which the Phase 2 clues were to be posted. The Phase 2 clues were as follows, and provided multiple paths to complete Phase 2 based on the contestant's preferred skills:

The Way of the Reverse Engineer

If you're used to getting down and dirty with a binary, a disassembler, and following code paths, this was probably the Way you went. Two different binaries were provided by Cody Pierce, each with a couple of different ways that you could uncover the goal.

The Way of the Lockpicker

If your best skill is lockpicking, you probably started hunting down jgor or a13k and got to picking! You can read about their Phase 2 challenge on jgor's website.

The Way of the Cracker

Have a massive password cracking farm at your disposal? Good at guessing passphrases? This Way, provided by Rick Redman over at Kore Logic, was likely your best bet.

The Way of the Network Analyst

Stare at packets all day? Know the ins and outs of packet format alignment and various encoding schemes? Tackling the pcap provided by Tod Beardsley was probably the Way to go. You can read about this Way in detail over in this imgur album.

The Way of the Cryptologist

Codes and ciphers your thing? You probably found your way over to pastebin and noodled on the crypto challenge provided by Dan Crowley from Trustwave. You can read about this Way in detail on the Trustwave Spiderlabs blog.

The Way of the Wireless Ninja

Best with waves that traverse the air? You should have gone up to Caesar's Roman tower, Floor 12 or so, and started observing the broadcasts from Dragorn's wireless challenge. We heard however that you could pick up the broadcasts from as far away as a few floors above and below 12 as well. You can read about this Way in detail over at Dragorn's blog.

Phase 2 Goal

The goal of all Phase 2 challenges was to uncover the email address "lawl.bitcoin@gmail.com", which upon emailing would begin Phase 3. Due to the manner in which Phase 2 was conducted, it's difficult to determine how many people went which Way, however we do have some confirmations on which Way was taken reported by the contestants themselves as they began Phase 3:

- Reverse Engineer: 29
- Wireless Ninja: ?
- Network Analyst: ?
- Lockpicker: 6
- Cracker: 3
- Cryptologist: 6
- Unknown: 26

If you completed one of the challenges that we don't have a statistic for, please let us know in the comments section so that we can update our data!

Phase 3: Bitcoin!

Emailing "lawl.bitcoin@gmail.com" would begin Phase 3, but only if you did so using encryption. If you emailed in plaintext, you would be instructed to use encryption. The PGP key for this email address could easily be

found on the keyservers. This step of the challenge was included to promote secure communications, spread awareness of PGP, and cause people who had never used it before to learn how to use email encryption.
Once using encrypted email to contact “lawl.bitcoin@gmail.com”, a unique Bitcoin address would be generated for you and you were instructed to pay 0.00031337 BTC to the provided address. This step required you to either obtain some Bitcoin and pay the address yourself, or at least know someone who could on your behalf. There were a number of ways to obtain BTC during the conferences, most notably our @LOLBitcoin Twitter fountain which dropped pre-loaded Bitcoin private keys at regular intervals, and the Bitcoin ATM Briefcase floating around the conferences and parties. This step of the challenge was included to spread awareness and promote the use of Bitcoin, and, well, it was thematically consistent with the theme of the party.
Upon paying the 0.00031337 BTC to the provided address, you were provided via email with a block of data and a unique passphrase, which began Phase 4. Once using encrypted email to contact “lawl.bitcoin@gmail.com”, a unique Bitcoin address would be generated for you and you were instructed to pay 0.00031337 BTC to the provided address.

Phase 4: Follow the Whyte Rabbit

The fourth and final phase began when receiving the following data after making a successful Bitcoin payment at the end of Phase 3, along with a unique passphrase:
aHR0cDovL3doeXRlcmFiYml0LmNvbS9y
YWJiaXRfPz8/Pz8/Lmh0bWwNCg0KSSBs
ZWF2ZSB0aGVzZSBiZWhpbmQNCndoZXJl
dmVyIEkgcm9hbQ0KZm9yIHRob3NlIHdp
bGxpbmcgdG8gc2VlayBtZQ0KdG8gZm9s
bG93IG1lIGhvbWUuLi4uDQoNCi13aHl
0ZXJhYmJpdA==
This BASE64 data decodes to the following plaintext:
http://whyterabbit.com/rabbit_??????.html

I leave these behind
wherever I roam
for those willing to seek me
to follow me home....

-whyterabbit
Phase 4 primarily involved tracking and hunting down the Whyte Rabbit. The Rabbit was not necessarily always the same person, but was the person currently carrying the Rabbit Bag which contained badges for the party, lanyards, some swag, and the Rabbit Phone. The Rabbit Phone was GPS tracked and configured with Twitter, Foursquare, and Instagram social media accounts.
If you haven’t figured out the solution to the riddle above yet, it’s “prints”. By plugging in “prints” in place of the question marks in the URL, the location of the Rabbit was uncovered as the URL pointed to a page that was constantly updated with the GPS coordinates of the Rabbit Phone, which could be used to fairly accurately track down the Rabbit, assuming the Rabbit was not in a casino or other large building where cell phone reception and GPS tracking becomes unreliable. As “prints” is only six characters, it is possible that the URL could have been brute forced if you were unsuccessful with the riddle, or on the primary index page, the rabbits left foot contains the string “stn1rp” which when read in reverse reveals “pr1nts” which hopefully was a good enough clue that “prints” is the answer to the missing portion of the URL. The GPS coordinates page

contained both GPS coordinates as well as a UTC timestamp. Some people missed the UTC time and thought it was telling them that the rabbit would appear at that location in the future. We had to add “UTC” to the time string to reduce confusion.
Any incorrect guess of the URL would redirect to the primary index page which contained some text as well as an ASCII image of the Whyte Rabbit. However, if you were unable to find the GPS coordinates page there were a few other Easter eggs this Rabbit left to be found on the primary index page:

Twitter

The Rabbit had a @_WhyteRabbit_ Twitter account that it would occasionally post to, or cross-post to from one of the Rabbit’s other social media accounts. On the primary index page, the string “_julgrenoovg_” could be found in the middle of the clock which is “_whyterabbit_” Caesar shifted by 13 revealing the twitter handle.

Foursquare

Even with only a general awareness of the Rabbit’s location provided by the GPS coordinates, the Rabbit provided many other clues as to their whereabouts such as check-ins on Foursquare under the _WhyteRabbit_ account. The Rabbit Phone was frequently checked into locations such as the Galleria Bar at Caesars Palace, various shops and casinos, and many other locations.

Instagram

Many times a Foursquare check in would be accompanied by an Instagram post of a picture of something nearby, from the vantage point of the Rabbit. These location contextual clues could be used to fairly accurately identify the location of the Rabbit. On the Whyte Rabbit website’s primary index page, the text string “h%2Ftm%2Ftbt%2Fa._eitigcwrtpnroha_%3Asamyb” could be found near the top. This required a URL decode and then a 5 character skip to get the URL to the Rabbit’s _WhyteRabbit_ Instagram page.

Rabbit Phone’s Phone Number

The favicon for the whyterabbit.com site was a simple image with green and black pixels. If you interpret the black pixels as 0 and the green pixels as 1, when read from left to right, each row is a set of 16 bits. This data revealed the Rabbit Phone’s phone number, which could be used to call the Rabbit Phone. Making the Rabbit Phone ring when in close proximity could reveal the location of the Rabbit, or if the Rabbit answered, perhaps you could have coaxed some additional clues out of them (:

Completing Phase 4

Once a contestant had found the Whyte Rabbit, they were required to give their unique pass phrase and confirm the email address they used in Phase 3. If both were correct, they received a badge to the party!