Pony's C&C servers hidden inside the Bitcoin blockchain

By Omri Herscovici

Published: 2019-10-17 · Archived: 2026-04-15 02:11:08 UTC

Research by: Kobi Eisenkraft, Arie Olshtein

Introduction

Redaman is a form of banking malware distributed by phishing campaigns that target mostly Russia language speakers. First seen in 2015 and reported as the RTM banking Trojan, new versions of Redaman appeared in 2017 and 2018. In September 2019, Check Point researchers identified a new version that hides Pony C&C server IP addresses inside the Bitcoin blockchain.

In the past we have seen others techniques that used Bitcoin blockchain to hide their C&C server IP address, but in this blog we will share an analysis of the new technique.

The malware connects to Bitcoin blockchain and chaining transactions in order to find the hidden C&C server, we called this new technique Chaining.

Infection chain

How the attacker hides the C&C servers in Bitcoin blockchain

In this real example the attacker wants to hide IP 185.203.116.47

In order to do this, the attacker uses wallet **1BkeGqpo8M5KNVYXW3obmQt1R58zXAqLBQ** :

1. The attacker converts each octet of the IP address from decimal to hexadecimal: 185.203.116.47 => B9.CB.74.2F

2. The attacker takes the first 2 octets, B9 and CB and combines them in opposite order B9.CB => CBB9

3. The attacker then converts back from hexadecimal to decimal, CBB9 ==> 52153.

- 0.00052153 BTC (about 4$) is the first transaction he will do to the **1BkeGqpo8M5KNVYXW3obmQt1R58zXAqLBQ** wallet

4. The attacker takes the last 2 octets, 74 and 2F and combines them in opposite order 74.2F => 2F74

5. The attacker converts back from hexadecimal to decimal, 2F74==> 12148.

- 0.00012148 BTC (about 1$) is the second transaction he will do to the **1BkeGqpo8M5KNVYXW3obmQt1R58zXAqLBQ** wallet

Figure 1 – Related transactions with amounts of 0.00052153 and 0.00012148 BTC
https://www.blockchain.com/btc/address/1BkeGqpo8M5KNVYXW3obmQt1R58zXAqLBQ?sort=0

How Redaman malware reveals the dynamic hidden C&C server IP

Redaman does the opposite to the algorithm described above.

1. Redaman send a GET request to get the last ten transactions on the hard coded Bitcoin wallet **1BkeGqpo8M5KNVYXW3obmQt1R58zXAqLBQ**

- https://api.blockcypher.com/v1/btc/main/addrs/1BkeGqpo8M5KNVYXW3obmQt1R58zXAqLBQ?limit=10

2. It takes the values of the last two payment transactions to Bitcoin wallets **52153** and **12148**.

3. Converts the Decimal values from the transactions to Hexadecimal 52153==>CBB9 and 12148==>2F74.

4. Splits the Hexadecimal value to low and high bytes, changes the order and converts them back to decimal. B9==>**185**, CB==>**203**, 74==>**116**, 2F==>**47**

5. These values together combine the IP address of the hidden C&C server IP **185.203.116.47**.

Figure 2 – The actual code that calculate the C&C server IP, you can see in “Dump 1” the hexadecimal values of the C&C server IP: B9 CB 74 2F (185.203.116.47)

Figure 3 – Json response that include the hidden C&C server IP

Conclusion

In this blog, we described how Redaman has become more effective by hiding dynamic C&C server addresses inside the Bitcoin blockchain.

In contrast to the simple C&C setups based on static/hard coded IP addresses that provide an easy way to defend against this type of attack.

Indicators of Compromise:

Hidden C&C servers

185.203.116.47	35.216.185.203	78.108.216.39	100.66.91.200	72.50.91.200
117.49.185.203	170.51.35.216	91.200.78.108	69.5.100.66	185.234.72.50
185.203.117.49	118.16.170.51	103.136.91.200	91.200.69.5	150.254.185.234
119.169.185.203	94.156.118.16	100.174.103.136	54.151.91.200	212.73.150.254

185.177.119.169	85.217.94.156	91.200.102.39	172.104.54.151	227.99.212.73
185.203.185.177	35.216.85.217	91.200.103.136	69.5.172.104	195.123.227.99
171.48.185.203	94.156.35.216	216.39.91.200	172.105.69.5	
59.149.171.48	119.18.94.156	100.134.78.108	100.134.172.105	
85.217.59.149	170.51.185.203	91.200.100.134	91.200.100.66	
119.169.85.217	85.217.170.51	100.136.91.200	195.123.91.200	
185.203.119.169	118.16.85.217	91.200.100.136	185.234.195.123	
85.217.171.48	185.203.118.16	100.134.91.200	72.50.185.234	
59.149.85.217	91.200.185.203	172.105.100.134	212.73.72.50	
185.177.59.149	100.174.91.200	54.151.172.105	100.136.212.73	
119.18.185.177	91.200.100.174	100.136.54.151	227.99.91.200	
185.203.119.18	102.39.91.200	172.104.91.200	150.254.227.99	
185.203.185.203	216.39.102.39	91.200.172.104	100.136.150.254	

Redaman samples

cf9c74ed67a4fbe89ab77643f3acbd98b14d5568

c098dc7c06e0da8f6e2551f262375713ba87ca05

3933f8309824a9127dde97b9c0f5459b06fd6c13

817bd8fff5b026ba74852955eb5f84244a92e098

51c7a774a0616b4611966d6d4f783c1164c9fa50

44b6627acd5b2c601443c55d2e44ae4298381720

d9fb2504008345af97b0e400706cdaa406476314

bbdce69acc6101c1f61748c91010c579625ef758

3f2b758122c0d180ccfba03b74b593854f2b0e86

9d7b264367320da38c94be1f940c663375d67a2a

Bitcoin wallet

1BkeGqpo8M5KNVYXW3obmQt1R58zXAqLBQ – The wallet is not recognized as malicious in any blockchain databases but Check Point incriminates it.
