Advenutures in Shellcode Obfuscation! Part 5: Base64

redsiege.com/blog/2024/07/advenutures-in-shellcode-obfuscation-part-5-base64

By Red Siege | July 18, 2024

by Mike Saunders, Principal Consultant

Watch Video At: https://youtu.be/Z6BWalaAKFE

This blog is the fifth in a series of blogs on obfuscation techniques for hiding shellcode. You can find the rest of the series here. If you'd like to try these techniques out on your own, you can find the code we'll be using on the Red Siege GitHub. Let's look at some methods we can use to hide our shellcode.

The Basics

One of the most basic obfuscation techniques we could use would be to Base64-encode our shellcode and embed that in our loader. Encoding our payload is a relatively simple process with Python using the following code:

```
import base64

plaintext = open('payload.bin', "rb").read()

b64 = base64.b64encode(plaintext)

print(b64)
```

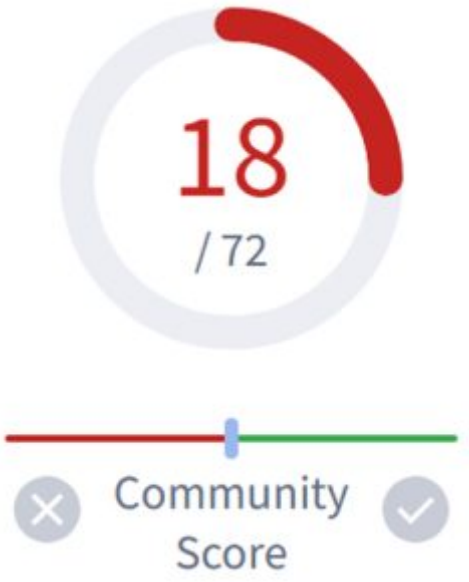
While I'll be using C for most of the proofs-of-concept for this series, I'll be using C# here as it provides a simple to use method of converting Base64-encoded data. To use our B64 string generated by the Python script, we first need to place it into a new `string` variable. After that, we can use `Convert.FromBase64String` to convert our Base64-encoded shellcode into a byte array. For this example, I'm using a relatively small Meterpreter `reverse_http` payload. If you were using a larger unstaged payload, like a Cobalt Strike beacon, it would probably be better to load the Base64-encoded payload from a remote server rather than embedding it into the executable as a gigantic string.

```
string s = "/EiD5PDozAAAA…";

byte[] shellcode = Convert.FromBase64String(s);
```

At this point, we could easily copy this byte array into a memory buffer and execute it. Checking the proof-of-concept program against VirusTotal shows this technique was detected by 18 engines, however, so it's probably not a great option.

As you can see, Base64 encoding is not an effective obfuscation strategy on its own. It is effective at helping lower entropy, however, so it could be used to encode high entropy encrypted data.



Base64 String Score

Try it Yourself

You can find the example code for this article as well as the other articles in this series at the Red Siege GitHub.

Stay Tuned

This blog is part of a larger series on obfuscation techniques. Stay tuned for our next installment!

About Principal Security Consultant Mike Saunders

Mike Saunders is Red Siege Information Security's Principal Consultant. Mike has over 25 years of IT and security expertise, having worked in the ISP, banking, insurance, and agriculture businesses. Mike gained knowledge in a range of roles throughout his career, including system and network administration, development, and security architecture. Mike is a highly regarded and experienced international speaker with notable cybersecurity talks at conferences such as DerbyCon, Circle City Con, SANS Enterprise Summit, and NorthSec, in addition to having more than a decade of experience as a penetration tester. You can find Mike's in-depth technical blogs and tool releases online and learn from his several offensive and defensive-focused SiegeCasts. He has been a member of the NCCCDC Red Team on several occasions and is the Lead Red Team Operator for Red Siege Information Security.

Certifications:
GCIH, GPEN, GWAPT, GMOB, CISSP, and OSCP

Related Stories

View More

Adventures in Shellcode Obfuscation! Part 7: Flipping the Script

By Red Siege | August 1, 2024

by Mike Saunders, Principal Security Consultant This blog is the seventh in a series of blogs on obfuscation techniques for hiding shellcode. You can find the rest of the series […]

Learn More
Adventures in Shellcode Obfuscation! Part 7: Flipping the Script

Out of Chaos: Applying Structure to Web Application Penetration Testing

By Red Siege | July 25, 2024

By Stuart Rorer, Security Consultant As a kid, I remember watching shopping contest shows where people, wildly, darted through a store trying to obtain specific objects, or gather as much […]

Learn More
Out of Chaos: Applying Structure to Web Application Penetration Testing

Adventures in Shellcode Obfuscation! Part 6: Two Array Method

By Red Siege | July 23, 2024

by Mike Saunders, Principal Security Consultant This blog is the sixth in a series of blogs on obfuscation techniques for hiding shellcode. You can find the rest of […]

Learn More
Adventures in Shellcode Obfuscation! Part 6: Two Array Method