Format Strings

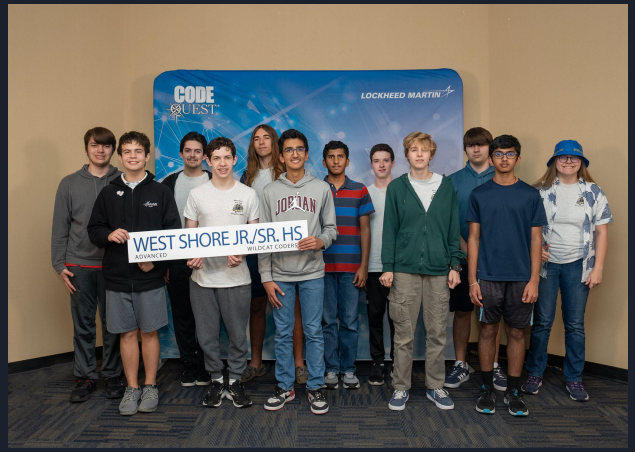
Level 0x08

Quick Overview

- Events / Planning
- VPNs
- Format Strings

Upcoming Events

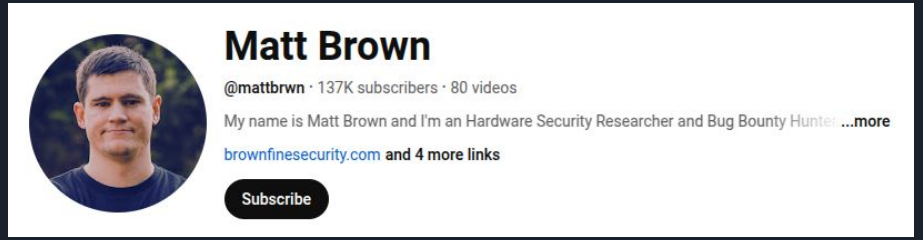
- Code Quest
  - Saturday, March 1
  - Teams are 2-3 people
- Spring Break. March 17-21st
- Cyber Quest
  - March 29
  - Teams are 3-5 students
- We need to setup teams and get a list of who is going



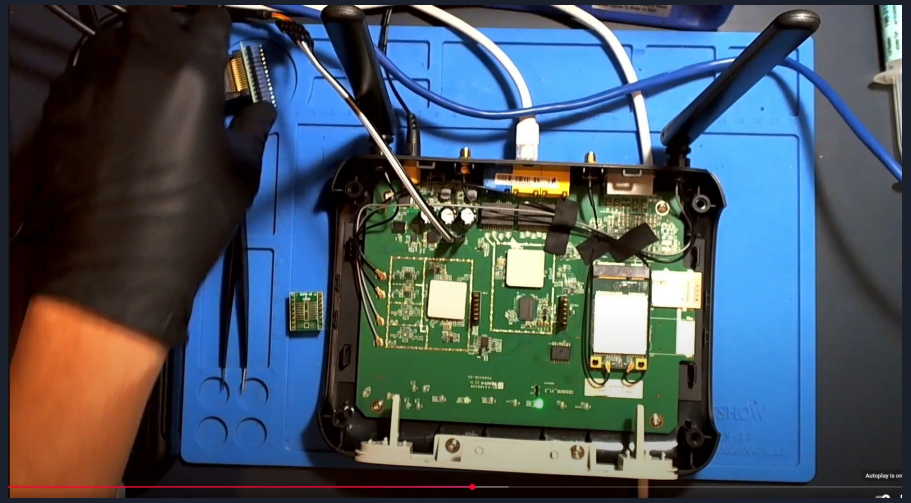
Future Topics

- Hardware hacking?
  - PoE IP Camera
  - GM or Toyota Head Unit
- NES game hacking?
  - Custom cheats / mods
  - Pwn Adventure Z
- Electronics
  - Intro to digital circuits
- Embedded
  - Arduino
  - Raspberry Pi
- Advanced programming concepts
  - Game design project
  - GUI programming
  - Rust
- Build PC from parts
- CTF Challenge authoring

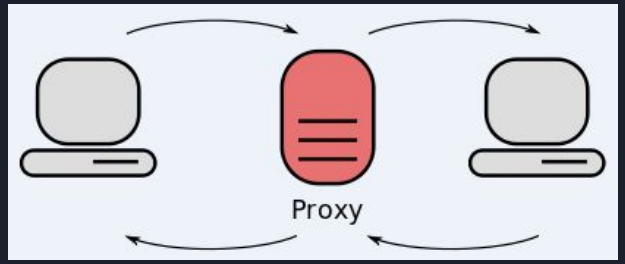
Matt Brown

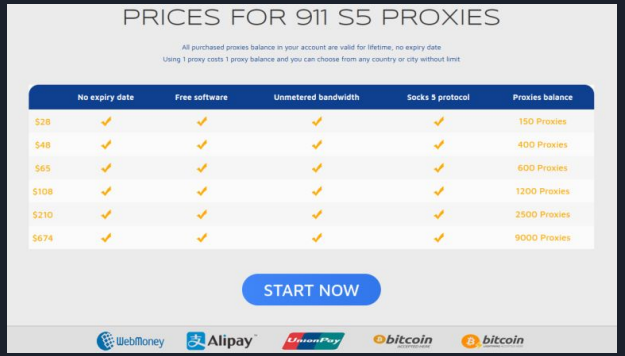


- Reverse Engineer
- Hardware Hacker
- Youtube Channel
  - Routers
  - License plate readers
  - Cameras
  - IOT Devices

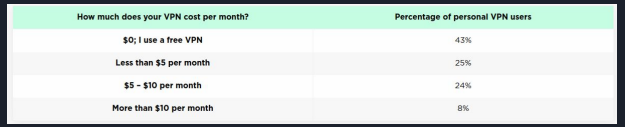


VPNs



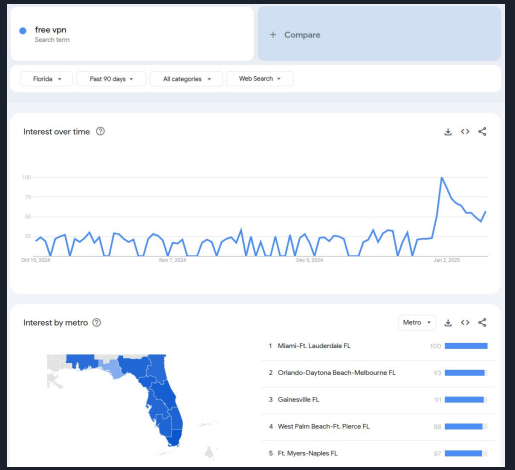


- What IP block never gets blocked / filtered by US businesses?
- Cyber criminals would love to use your IP address
- States / countries with content geo restrictions driving VPN usage worldwide



How much does your VPN cost per month?	Percentage of personal VPN users
$0; I use a free VPN	43%
Less than $5 per month	25%
$5 - $10 per month	24%
More than $10 per month	8%

- 911 S5 botnet had 19 million PCs infected in 190 countries
- Free VPNs: MaskVPN, DewVPN, PaladinVPN, Shield VPN, ShineVPN
- Free game cracks / pirate software
- Big Mama VPN



Format Strings

- Normal C format string / printf usage:

```
printf("Hello World\n");
printf("We can print variables test = %d or constants = %d\n", test, 1234);
printf("%s has %.02f dollars at %s\n", user_name, balance, bank_name);
```

- First parameter is format string
- Format string can contain format parameters

  `%s` for a string

  `%d` for an integer

  `%f` for a floating-point
- Each format parameter requires coder to add a parameter to function call

Format String Bug

- To print a single string using printf you should:

```
printf("%s", my_string);
```

- It is bad practice to use your variable as the format string directly

```
printf(my_string);  // technically works, but bad
```

- It is a huge vulnerability to let a user control a format string:

```
char buf[100];
printf("What is you name?\n");
fgets(buf, 100, stdin);   // User can set the value of buf
printf("Your name is: ");
printf(buf);   // User controls the format string!!!  VULNERABILTY
```

Exploitation

- User can create a format string with format parameters:

```
My name is %08x %08x %08x %08x
can also print out strings %s %s %s %s
```

- Above format string will print out the value of 4 function parameters as hexadecimal
- Function parameters are determined by ABI / calling conventions of libc
- Can print out CPU registers or stack contents
- Memory read vulnerability
  - Stack cookies
  - Pointer addresses / defeat ASLR
  - Other variables in memory

Calling Conventions

How arguments are passed to functions:

Argument Number	x86 cdecl (Linux)	x86 fastcall (MS)	AMD64 (Linux)	AMD64 (MS)	ARM32
1	stack / push	ECX	RDI	RCX	R0
2	stack / push	EDX	RSI	RDX	R1
3	stack / push	stack / push	RDX	R8	R2
4	stack / push	stack / push	RCX	R9	R3
5	stack / push	stack / push	R8	stack / push	stack / push
Return value	EAX		RAX	RAX	R0

Special Format Parameter

- The %n format character is very unique
  - It writes to a pointer (memory address) the length of the string
  - Used for determining how long a string is
- Example usage:

```
int name_len = 0;
printf("%s %s%n\n", "Michael", "Wales", &name_len);
printf("Your name is %d bytes\n", name_len);
```

- Causes a memory location to be written to

Format Vulnerability with %n

- If user has access to format string, can write arbitrary values to memory
- Attacker can control how long string is before %n
- Attacker can control what memory address / register
  - Add %d format parameters before the %n to change register / stack offset
- Attacker can easily create long strings through format parameters:

  `"%20s %n"` // will write a string 20 bytes long, and then a 21 to the next parameter

Attributions

- https://krebsonsecurity.com/2024/05/is-your-computer-part-of-the-largest-botnet-ever/
- https://www.security.org/resources/vpn-consumer-report-annual/
- https://www.youtube.com/watch?v=ugaLp6BIkgo Low Level on YouTube