WE DON'T KNOCK

Miscreant Crèche

Balancing Risk, Benefit and Education

The Risk

The Short Version

This document covers the risks of the Miscreant Crèche from the perspective of putting skills for covert entry and "hacking" into the hands of the general public. This risk has been considered carefully and significant limitations placed on the technical difficulty of the activities and the tools in use.

The Long Version

The concern is justified – are we teaching covert entry and ways of bypassing security systems to the general public? The answer is both yes and no.

Significant limitations have been placed on what techniques are to be covered. The marketing literature makes it clear that **only certain devices will be supported** with instruction (Flipper Zero). Whilst people are welcome to bring more advanced equipment (e.g. a Proxmark), no instruction will be given. This sets the boundary between **off the shelf educational tools** which **do not exploit any new security vulnerabilities** (attacks using a Flipper Zero have had better equipment available for around a decade) and professional equipment used by highly technical covert entry teams and security researchers (e.g. the Proxmark).

Consideration has also been given to the kinds of activities on offer. Where access control systems are used, there is a **significant and intentional gap** in the technologies. Some are based on **early 1990s technology** which is **no longer considered secure** (it really never was). Then there is a step up to **mid-late 1990s era** which is still in use in some **low security environments** and has a whole range of vulnerabilities which are well known and easily exploited with a range of tools. We then **leave a significant gap** and jump to very modern, unbroken encryption standards. This gap means we are **missing out more modern, in-use technologies** in higher security areas.

This is just the access cards. The same approach is taken with the underlying **communication technology**, which uses the standards **from the 1970s** and **not modern OSDP standards**.

The Risk

A similar approach is taken with radio attacks. We have **basic static code systems** which are, again, **from the 1990s** and of use only for turning on remote controlled lights. Where rolling codes systems are used, these are simulated and a specific range of attacks used. Again, **better equipment has long been available to criminals**.

The Benefit

The Short Version

Controlled curiosity and education. We want people to be aware of what makes good security and we want them to discover it in a way that doesn't cause mischief and inconvenience or result in people getting a criminal record for their curiosity.

The Long Version

The kinds of people who have bought these tools have bought them to **explore, test and generally be curious**. They're usually creative and curious people. The problem is that, in order to satisfy that curiosity, **people have often had to break the law**. This **brings attention** to **manufacturers using unacceptable security** and just hoping people don't notice.

Miscreant Crèche is **inspired by the cyber security space**, where online services exist allowing people to log into remote computers and try hacking them. This has many benefits from training to ensuring people who are just curious and want to test themselves don't have to bother the FBI.

Very simply – **if the Flipper Zero can compromise the security of your home or workplace, you want to know about it**. The criminals have had the capability for years. **Education of the public** as to what makes good security will make our lives as adversarial security professionals harder, but **makes everyone safer.**

Enquiries@StyxSecurity.org

We don't knock.

Summary

We recognise there will be concerns around the Miscreant Crèche. It's the kind of niche activity that appeals to a specific kind of person and tends to worry some other people.

We've taken great care with the activities we are putting on and we are explicitly **not providing training** in the conventional sense. We are providing an environment for people who have bought these tools to use them without bothering others.

If you are still worried, I would point you towards locksport. This has been around for a long time and is the picking of locks as a hobby / competition. People are testing and demonstrating their skills and capabilities in a controlled manner. For them it is a puzzle, not a means of breaking in. It's actually quite prolific.

Yet we don't see much lock picking in the real world, outside of high end industrial espionage or government backed covert activities.

The biggest risk is the intent of the people attending. "Hacker-types" are very easily identifiable with a very specific set of personality traits. We define "hackers" in the sense of creative, curious problem solvers. The specific traits we look for are technical, research-based and not going to be discussed outside of NDA, as it's our main screening tool for this and other such interactions.

They are very different to the usual criminal and it's almost impossible for a criminal to convincingly replicate these traits. Any criminal with the hacker mindset and criminal intent would be highly unlikely to need or want to attend an event like the Miscreant Crèche.

Assessing personality types and intent is part of the bread and butter of a security company. Anyone who we think might be just trying to learn how to break into places will be asked to leave.

If you have specific concerns or want more technical information on the specific activities or technologies in use, please contact us on the email address below.

Enquiries@StyxSecurity.org

We don't knock.