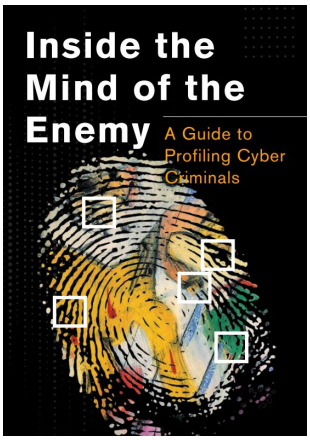
CounterCraft

carahsoft.



Inside the Mind of the Enemy

A Guide to Profiling Cyber Criminals

Thank you for downloading this CounterCraft eBook. Carahsoft is the distributor for CounterCraft Cybersecurity solutions available via NASA SEWP V, ITES-SW2, NCPA & OMNIA Partners Company, and other contract vehicles.

To learn how to take the next step toward acquiring CounterCraft's solutions, please check out the following resources and information:

For additional resources:
carah.io/countercraftresources

For upcoming events:
carah.io/countercraftevents

For additional [vendor] solutions:
carah.io/countercraftresources

For additional Zero Trust solutions:
carah.io/countercraftsolutions

To set up a meeting:
countercraft@carahsoft.com
888.662.2724

To purchase, check out the contract vehicles available for procurement:
carah.io/countercraftcontracts

For more information, contact Carahsoft or our reseller partners:
countercraft@carahsoft.com | 888.662.2724

Inside the Mind of the Enemy

A Guide to Profiling Cyber Criminals

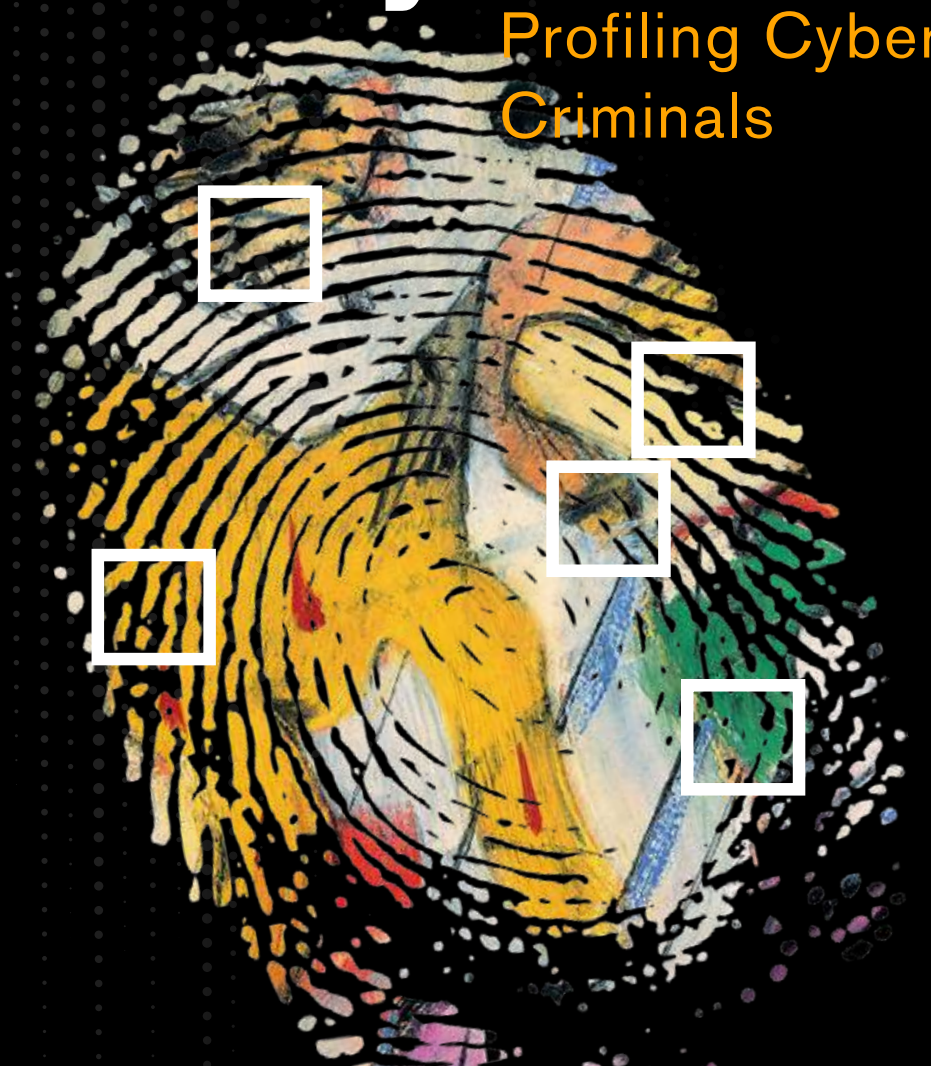


Table of Contents

> **The opportunity to secure ourselves against defeat lies in our own hands, but the opportunity of defeating the enemy is provided by the enemy himself.**

- Sun Tzu, The Art of War

Intro

In this ebook, you will find a comprehensive look at how criminal profiling is useful in cybersecurity. We will start by looking at the concept of criminal profiling and what it can help predict. Then, we will take a closer look at how profiling can be of use to security practitioners in all aspects of their work and be a really useful tool in every cybersecurity expert's belt.

After all, we spend our days working to make the digital world a safer place, so taking time to understand who we are dealing with is a really useful process. Have you ever thought about what motivates a cyber criminal? The answer may often be money, but to stop there would be oversimplifying things.

It's important to remember that profiles are not an end in themselves. An adversary profile is usually created from behaviour patterns collected from the deception environment. This provides valuable information about who is attacking, but the profile can also be used to plan and design your deception deployment by allowing the plan to focus on specific characteristics of the adversary.

Cyber deception is one of the only defense tools that actually helps in the process of profiling, so we will take a close look at how it manages to do so in the following chapter. Finally, we will wrap up with a review of the objectives and how to use the profile we create.

We hope you find this ebook useful,

Richard Barrell and the team at CounterCraft

What is Profiling?

The FBI refer to profiling as ‘reverse engineering a crime’ - the process of analyzing a crime scene to build a picture of the criminal, ultimately leading to an arrest. Criminal profiling is used to describe an overarching approach to criminal investigation.

We can say criminal profiling consists of an analysis of behavior patterns that can help predict several things about a person who has committed a crime:

1. Their personality traits
2. Their modus operandi
3. The motivation to commit the crime
4. Potential future steps

Why do criminologists employ profiling? The main goal is to not only understand the enemy, but also to reach an understanding that will allow preventative measures to be put into place.

Cyber profiling

In cyber terms, profiling is a process of identifying individual characteristics and traits displayed by the adversary. This ebook will show how we can profile cyber adversaries using deception technology.

A cyber criminal profile is essential in order to learn how attackers think, what motivates them and how they work. Cyber criminals are intelligent, highly skilled and usually very resourceful, making it difficult, but not impossible, to catch or anticipate them. Understanding the enemy is the first tool used when fighting against them and cyber deception plays an important role.

Cyber crimes are based on exploring new ways of intrusion, new vulnerabilities and not getting detected, so often organizations aren't even aware they have been compromised. As our world gets more and more connected, companies large and small have more and more doors open to attacks. This means they are exposed to an infinite amount of highly complex threats that can affect and compromise a large variety of assets. Using an innovative approach and knowing how the enemy operates, what their techniques are, and their profiles is the key to fighting against them.

Profiling in context

When tracking a serial killer, the FBI looks for characteristics they can use to identify the murderer. They base the profile on the how and when of the crime, and use detailed analysis of the crime scene to enrich the data they gather.

Characteristics such as the choice of victim, where the crime took place, the level of organization of the killer, the time taken and post crime behavior, the sophistication of the crime, and the choice of weapon all provide important data about the motives, tools, techniques and procedures of the criminal. In the same way, we build profiles of cyber adversaries to build a picture of their objectives, modus operandi, and ultimately their future intentions.

Another example of using telltale fingerprints to profile an adversary comes from the Operators at Bletchley Park, once the top-secret home of the World War Two Codebreakers, who were able to identify U-Boot radio operators by the way they keyed their messages. On some occasions, they were able to identify troop movements just by how the Operators changed. The "Ultra" intelligence produced, including the criminal profiling done, is estimated to have shortened the war by two to four years, with some historians going as far to say that without it the outcome of the war would have been uncertain.

The Cyber Criminal Profile

But what are these criminals like? Based on Rashmi Saroha´s report Profiling a Cyber Criminal[1] the characteristics of the cyber criminals can be divided into four groups:

- Technical know-how
- Personal traits
- Social characteristics
- Motivating factors.

For this report, Saroha asked 20 psychology and sociology students to describe the personality and characteristics of cyber criminals. The resulting words that describe these types of criminals are

- Sharp
- Well-trained
- Strategic planners
- Resourceful
- Passionate
- Determined
- Marginalized
- Seeking monetary gain
- Greedy
- Strong political beliefs
- Intolerant and control-freak

We know our adversaries are smart, determined, highly technical and resourceful, but how can we use what we know to learn their individual style and objectives? In the Cybercrime Psychology – Proposal of an Offender Psychological Profile Report[2], Jakub Lickiewicz said that a specific characteristic of cyber crimes is “a scene of crime without a scene of crime.”

---

[1]Profiling a Cyber Criminal (Saroha, Rashmi; 2014)

[2]Cyber Crime Psychology–proposal of an offender psychological profile (Lickiewicz, Jakub; 2011)

Lickiewicz´s study explains that there are different factors that have an influence on the cyber criminals, such as:

- Biological factors
- External environment
- Intelligence
- Personality
- Social or technical skills.

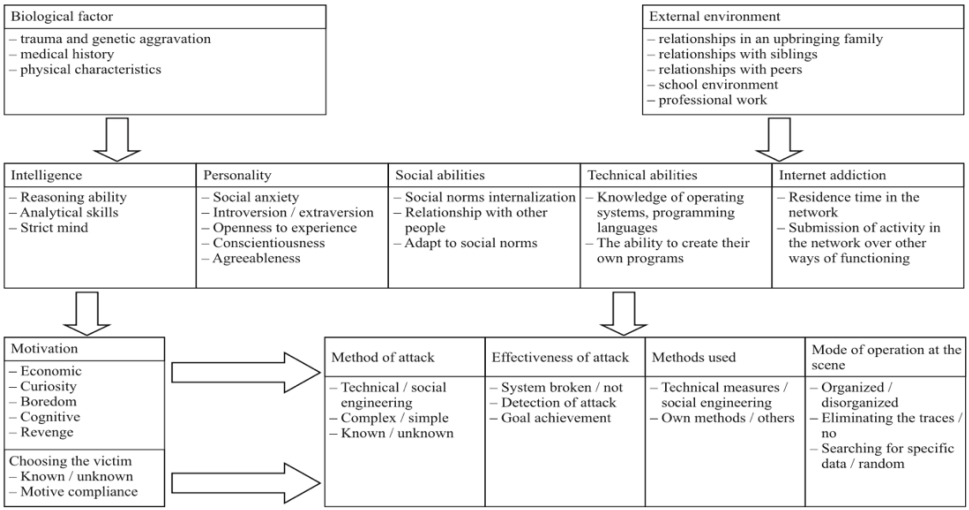


Figure 1: Theoretical model profile of a cyber criminal (Lickiewicz, 2011).

According to Solomia Fedushko, from Lviv Polytechnic National University; and Natalia Bardyn from the Ministry of Internal Affairs of Ukraine[3], typical motives to commit a cybercrime are:

- **Striving to demonstrate courage, bravery and firmness**
- **Absurd and dead earnestness that is expressed in a reckless, socially dangerous act**
- **Selfish attitude toward the harassment subject**

Meanwhile, reports show that there are varying motivating factors for different criminals and they should be considered when designing cybersecurity strategies. Three of the most common motivating factors are:

- Hackers and mafias motivated by financial gain and quick profits
- 'Hacktivists' who have strong political motivation
- Cyber criminals or networks of government-sponsored hackers who carry out cyber warfare.

The internet grants criminals anonymity—however, that does not mean their modus operandi, motivation and signature can't be recognized.

Computer crimes are often serial crimes, so, with the right cybersecurity tools and team with the ability to identify and understand the profiles and behavior, it is possible to determine the profile of the offender or the threat actor, as some cyber criminals have their own techniques and procedures.

[3]Algorithm of the Cybercriminal Identification (Fedushko, Solomia and Bardyn, Natalia; 2013)

How Profiling is Useful

Profiling can be incredibly useful in our fight against cybercrime. However, let's be clear: we're not talking 100% guaranteed attribution here. Profiling is not about getting the name, address and social security number of an adversary— that is a whole different story.

> What we can expect from profiling is the process of gathering a body of evidence that matches observed activity with known traits related to a given adversary.

A good profile provides valuable awareness in four areas:

- **What has the adversary been able to do?**
- **What are their objectives?**
- **Who are they?**
- **What are they going to do next?**

This is vital situational awareness that only real-time threat intelligence can provide.

With this data, you can respond effectively to any attack with the confidence that your response is correct and justifiable based on the threat you have identified. That means you can be sure that the response is the right one at the right time.

How Can Cyber Deception Technology Help Identify Threat Actors?

Criminal profiling is an art and a science. It calls for a certain level of strategic thinking, and in that way it shares much in common with cyber deception. Cyber deception technology and playing the same rules of the game as the adversaries currently stands out as a powerful approach to dealing with them and getting to know their intentions.

Although the identification of a threat actor is complicated, using sophisticated cyber deception techniques can help threat hunters create profiles of cyber attacks and gather as much information as possible about them. This can be done while simultaneously manipulating their surrounding environment and controlling what they have access to. Organizations are thus able to know what kind of threats they are facing and how to improve their security.

For Charles Fowler, former Chairman of the Defense Science Board, and Robert Nesbit, Former Senior Vice President of the Center for Integrated Intelligence Systems (CIIS) at the MITRE Corporation, deception should.

- have realistic timing and duration
- be integrated within the operation
- provide the concealment of true intentions
- be tailored to the needs of the setting.
- It also requires a degree of creativity and imagination to anticipate the cyber criminal.[4]

High-end cyber deception technology can be an ally for your organization when dealing with different kinds of adversaries.

---

[4]Demystifying Deception Technology: A Survey (Multiple Authors,2018)

How CounterCraft Helps You Profile an Adversary

The key to profiling an adversary is the ability to detect and collect their activity from the deception environment in real-time. This is exactly what we do at CounterCraft and what our solution detects, responds to and uses to get insights about your adversaries.The CounterCraft Deep Sense™ Agent captures all adversary activity from the deception host. It is able to relay this data via the ActiveLink™ command and control to the Deception Director in real time. As has been discussed elsewhere, this data is converted into event data.

Event data is actionable, timely and accurate threat intelligence. We use the event data as the foundation of the adversary profile. The following section describes how event data can be exploited.

IP Addresses and other Indicators of Compromise (IoCs)

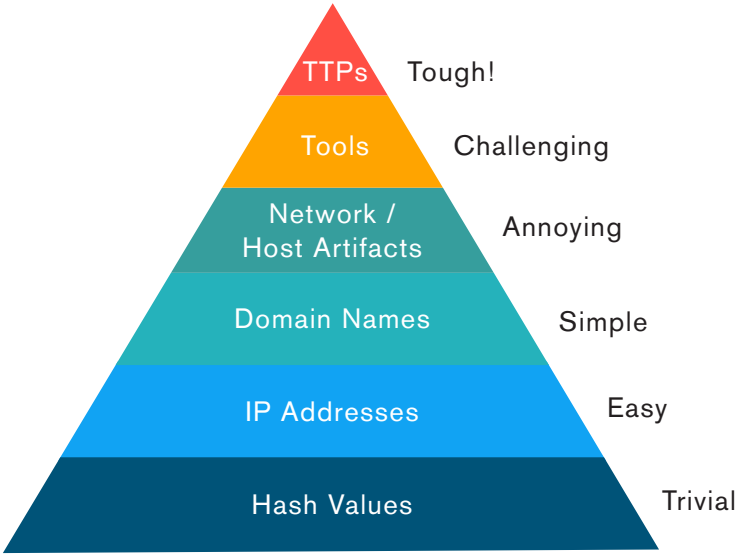
IoCs are extremely useful for linking to known threat actors. Event data is parsed to extract key observables. These observables provide really useful IoC data, such as IP address data or command arguments. As an example, the CounterCraft Threat Actor database contains hundreds of IP addresses that are linked to known APTs. Identifying a source IP address is an important adversary characteristic. Linking to the CounterCraft Event enrichment data allows you to obtain a wealth of information about the adversary.

You may be thinking that IP addresses can be spoofed, and are easy to change. While that is true, it's still a good technique to take any IP address detected within a deception environment and pipe it directly into your SIEM. If you detect the same IP address anywhere else in your network, you have direct evidence that that machine is compromised.

In addition, the CounterCraft Deception Director has access to external data feeds that can be used to enrich this data and enhance the power of their threat intel. In the case of IP addresses, we can automatically provide geo-location data; identify if this IP address is linked to any previous malicious activity or if it is a known Tor-node.

Patterns of Behavior & TTPs

We are creatures of habit. We all have our own ways of doing things, and cyber adversaries are no exception. David Bianco introduced the concept of the Pyramid of Pain in 2013 (which we talk about here) to quantify this. In a nutshell, changing the hash value of a payload is trivial, but changing the tools or TTPs from attack to attack is really challenging.



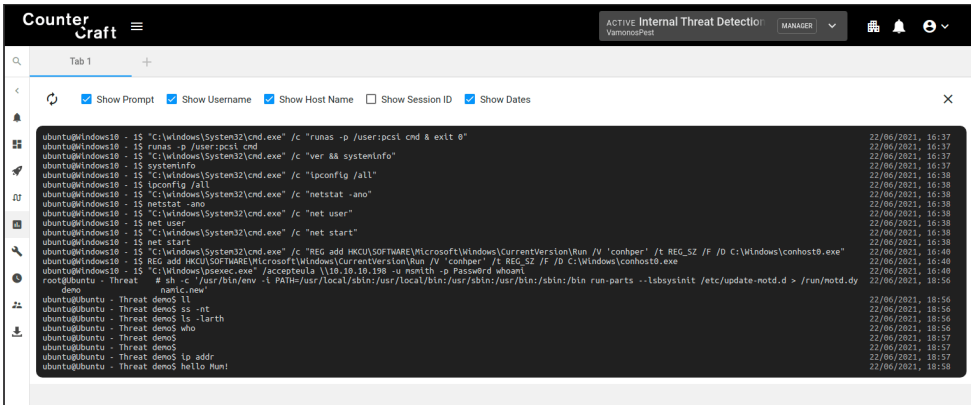
Changing the tools or TTPs from attack to attack is really challenging.

Even red teamers are an example of this concept. Each member of a red team typically has their own set of tools, their own penetration methods and their own sequence of actions that they perform to try and compromise a system.

By cataloguing these characteristics, you have a powerful way to identify an adversary, even to the point of identifying a specific individual by their characteristic tools, techniques, tactics and procedures.

The CounterCraft Shell-Line event type is a specific tool that is a real help with identifying unique adversary behavior by providing specific detail on what commands are being executed on the deception host. This can include, for example, everything that is executed through a bash shell - mistakes and all. Similar coverage exists for Windows hosts too.

By monitoring the commands used by an adversary, you can tell a lot about them: how familiar are they with the OS, or distribution; do they use specific command arguments (ps -faux, netsat -upanto etc), do they always use commands in the same order; do they make frequent mistakes?



Shell-line screenshot, showing mistakes and command usage.

By profiling the commands and techniques an adversary uses, and by noting their quirks and idiosyncrasies, it makes identification of this adversary much more likely if they are spotted again. You can only get this sort of attribution by monitoring adversary behavior, and the best way to do this is within a deception environment.

Identifying Objectives

Identifying the attack objective is an important part of the adversary profile. Is this just an opportunist who got lucky or is this part of a focused criminal attack aimed specifically at your organization? Using deception is a unique way to identify an attacker's objective.

By creating deception campaigns with attack trees that provide the adversary with choices, you can gain valuable intelligence from how they respond:

- ☐ DOS or data?
- ☐ Do they go for the user data?
- ☐ Do they go for the tactical data?
- ☐ Do they go for the IP or production data?
- ☐ How long do they spend in a particular area?
- ☐ Do they ignore everything and just upload a malicious payload?

You can use these observed behavior patterns to identify how the adversary prioritized their actions, and combine this with the IoCs and TTPs deployed to see how the tools they use advance their goal. You can also measure the time taken in different areas to judge the importance to the attacker.

What Next? Using the Profile

Up to this point, we've discussed various tools to help you profile your adversary. The question now is, how do we use this profile?

As we discussed before, a profile provides answers to the four key questions:

– What has the adversary been able to do?

– What are their objectives?

– Who are they?

– What are they going to do next?

These questions provide you with the awareness of the situation to respond effectively. The response may be a change in a configuration or a modification to a security policy or an update to user training. It could also be an automatic change by setting up rules to trigger on a specific behavior pattern to manipulate the adversary within the deception environment. Or it could be a link to an orchestration platform to initiate a response in the wider security ecosystem.

Whatever the response, by having a good understanding of the activity, motives and identity of the adversary gained from profiling techniques and data gathered from your deception environment, you can predict with greater confidence what they are going to do next and defeat them. And that is how we, as security professionals, can truly make a difference in cybersecurity.

Richard Barrell is the Product Manager at CounterCraft, as well as managing projects in the Government sector. You can find him on LinkedIn.

Security you don't expect.