Cyber Deception 101 – a primer on the subject

CounterCraft

For the majority of people, Cyber Deception is a new topic, and is probably not one that you would think of finding out about in most job roles.

This primer seeks to describe in outline why, if you are an Information Security professional, Cyber Security practitioner or Information Assurance team member you will want to know what it represents as part of your defence in depth approach to securing your organisation's information assets and systems.

Deception has been part of the make up of human history and the natural world we inhabit, and has enabled survival and defence objectives to be met in many areas.

In the 21st century the understanding and reality of an ever increasingly digital dependent society and business has ushered in the era of Cyber Deception. As in previous times deception can be used in both an offensive and defensive manner to achieve goals and objectives.

At CounterCraft we are focused on the technologies and techniques that matter in Defensive Cyber Deception.

An Opportunity to Re-balance the Asymmetry in Cyber Attack & Cyber Defence

Cyber Deception has been evolving over the past 20 years, not surprisingly in the military and intelligence communities, but over the past 5 years has begun to be adjusted and evolved to be a new approach in Enterprise Cyber Defence programmes. It has reached this stage due to the increasingly complex and growing threat landscape with cyber adversaries, many focussed on cyber crime are finding new ways of accessing corporate information systems and stealing intellectual property and misappropriating money.

These attackers use deception all the time to access systems, and that capability can now be used against them by defenders in an intelligent manner to prevent and disrupt the attackers ability to access their systems.

This is not about hacking back – it is about intelligent active defence in your own corporate environment.

Evolution of Honeypots & Honeynets to Full Enterprise Cyber Deception

Some readers will have heard of the honeynet project which has created an understanding and set of open source tools focussed on defensive cyber deception. From that pioneering work companies such as CounterCraft have been evolving and investing in scaling and hardening products and platforms to meet the needs of hard pressed enterprise cyber defence teams in their continual battle to keep the threat actors away from their systems and information assets.

At CounterCraft we have developed our own architectural and professional services approach to providing solutions to customers who are looking to add Cyber Deception to their approach.

What Makes Cyber Deception Different From Previous Cyber Defence Approaches?

For the past 30 years enterprise Chief Information Security Officers and their Enterprise Security Architects, if they existed, bought and built solutions which were all about "keeping the bad guys out" in a very overt and straightforward manner, and the industry evolved through the vocabulary of IDS, IPS, Firewalls, Cryptos, Anti-virus, Security Information & Event Management (SIEM), Cyber Threat Intelligence, Cloud Access Security Brokers, Security Automation & Orchestration. All of these technologies and approaches still deliver value and should keep about 80% of the attackers out.

What of that other estimated 20% (don't be surprised by pareto principles appearing in Cyber!)

These attackers can be classed as determined, motivated or persistent, and sometimes only occasionally advanced & persistent. They often find ways into organisations and their systems.

This is where the value of **Defensive Cyber Deception** really comes into its own as it enables defenders to design, build and operate synthetic and fake environments that fool the attackers into thinking they are accessing real production environments. **As a result they give away details of their Tactics, Techniques and Procedures (TTPs).**

With this information it is possible to carry out a number of valuable defence enhancing activities at different levels of an organisation:

1. The CISO has detailed intelligence on real attackers and what they are interested in accessing in the business. They can use this to inform future defence posture and investments, and talk to the board and peer C-Suite executives in a pre-breach environment
2. Enterprise Security Architects can deploy deceptions to improve the protection of certain information assets – sometimes termed Crown Jewels
3. Real-time information from a deception environment can be integrated machine-to-machine in a Security Operations Centre with SIEM and Threat Intelligence Platforms to enhance triage and threat hunting disciplines at a minimum
4. Bad guys may be deterred as they are wasting time on Fake rather than real assets

The list of potential value can be quite long – but hopefully this primer leaves you better informed and keen to embark on learning more about CounterCraft and our products.

Learn more about CounterCraft deception

Feel free to download our latest documents at countercraft.eu or contact at

craft@countercraftsec.com

About CounterCraft

CounterCraft, established in 2015, headquartered in San Sebastian (Spain), is an award-winning developer of the pioneering, deception-based cybersecurity platform for enterprise active cyber defense. This is combined with leading-edge research, technology and threat intelligence approaches, to enable CISOs to automate deception campaigns that push back against cybercrime. Powerful visualization and reporting, coupled with an advanced API suite, have won adoption by government, law enforcement, finance, retail, industrial, and Fortune 500 customers. CounterCraft is backed by leading VC firms, is a GCHQ Cyber Accelerator Alumni and operates globally.