Prescriptive Risk Solutions, LLC

March 2017

CISO Series on Today's Critical Issues

Honeypots & Cyber Deception

By Tari Schreider C|CISO, CHS-III, CRISC, ITIL™ v3, MBCI, MCRP, SSCP

Chief Cybersecurity Strategist & Author

Prescriptive Risk Solutions, LLC.

EC-Council

http://ciso.eccouncil.org/

What is a Honeypot?

There are few legal or shall I say quasi-legal ways to protect your information and assets offensively. Honeypots are one of those ways that organizations can go on the offensive against hackers and other cyber miscreants. If you have ever been duck hunting, you know how effective decoys can be in attracting game to the blind for the kill. Honeypots are no different, just a bit more high-tech.

Honeypots are servers, laptops, web-facing applications or other technology decoys setup to gather information about intruders targeting your company. Deploying decoys inside, outside the firewall, or within the DMZ simulate easy prey for hackers. The honey in these pots are simulated organization crown jewels such as financial reports, customer records or anything that a hacker would find attractive to exfiltrate. Once the intruders breach the honeypot, the trap is sprung. The honeypot monitors and records their actions.

ARE HONEYPOTS LEGAL?

By their very nature, honeypots detect illegal activities or in other words, they bear witness to attempts or commissions of crimes. What is your legal obligation to report this? Ironically, hackers have rights as well and the use of a honeypot may violate their Fourth Amendment rights. Is recording and capturing hacker activities considered illegal search and seizure? Honeypots have fewer security controls and run the risk of compromise. Untended honeypots configured by hackers as a botnet launching pad could harm others. What is your liability in the event the honeypot does harm to others? The Federal Wiretap Act prohibits the sniffing of electronic communications in real-time. What honeypot policies are in place to avoid violations of the Act?

Your organization's legal department should resolve these questions and others.

You should never embark on a honeypot project without advice of legal counsel.

ARE HONEYPOTS EFFECTIVE?

The sole determination of a honeypot's effectiveness is whether they fooled or disincentivised attackers from going after your organization's information. Were you able to take the information learned from the honeypot and buttress your organization's cyber defenses and countermeasures to thwart a similar attack? If the answer is yes, then if proved successful.

The effectiveness of a honeypot can only be determined in the context of intelligence gathering. They are not a prevention tool, but rather a method to understand the behavioral aspect of hackers. Honeypots provide valuable time for you to prepare for an attack when hackers are distracted when their attentions turn toward your honeypot rather than their desired target.

You can also determine the success of a honeypot through metrics gathered through your log management or security incident and event management (SIEM) system. These systems generally come with honeypot analytics rules that you can use to gauge the attractiveness of your honeypot and determine what type of information the attackers craved.

The most effective honeypot implementations are those deployed as a honeynet (multiple honeypots). Larger, complex networks will require multiple honeypots to produce enough useful information. Here the honeynet can actually simulate a production environment making it highly attractive to hackers. Using a SIEM to aggregate and correlate probes and attacks on the honeynet can yield valuable intelligence on attacker techniques, times, and motivations.

The SANS Institute InfoSec Reading Room offers an excellent paper entitled **Catching Flies: A Guide to the Various Flavors of Honeypots** written by Scott Smith. Check it out.

WHERE TO FIND HONEYPOTS

GitHub maintains a curated list of honeypots and related tools. The vast majority are open source, free codebases or donation-based products.

Presentation of their list is in the following sections:

- **Honeypots**
- **Honeyd Tools**
- **Network & Artifact Analysis**
- **Data Tools**
- **Guides**

You will quickly see that with hundreds of options available, selecting a honeypot can become overwhelming. There are however, available commercial systems that you may acquire along with professional services to deploy an effective honeypot.

The following are some of the more popular commercial solutions:

HONEYPOT	OVERVIEW
Canary	Intended as a honeynet, Canary's, are designed to solicit further investigation from hackers, at which point your Canary notifies you of the incident.
HoneyPoint Security Server™	Patented platform of distributed honeypot technologies.
KFSensor	Established 12-year old product that acts as a honeypot, designed to attract and detect hackers and worms by simulating vulnerable system services and Trojans.
Spector	Smart honeypot-based intrusion detection system.

A new generation of honeypots known as deception technologies that take the concept of a honeypot to an entirely new level has emerged.

CYBER DECEPTION

If you have decided to go the route of the honeypot, you should also consider adding a little deception to the mix. An emerging technology known as cyber deception, depceptionware or high-interaction honeypots is changing how we look at active defenses. Cyber deception is designed to dangle bait in front of would be attackers, luring them into a sandbox to study. Attackers are deceived in thinking; the sandbox is an actual production network with tasty data morsels to steal. While in the sandbox, the attacker is surveilled and fingerprinted.

Fingerprinting is the process of capturing the attacker's movements, techniques and observable patterns of attack. One of the key strategies is to get the attacker to deposit a malicious payload and exit the sandbox so that their malicious code can be analyzed and protective measures applied to the real network. A focus of these products is something referred to as east-west or lateral attacks (inside the network).
The following are currently available cyber deception products:

COMPANY	BOUNTY
CyberTrap	Interactive deception technology to lure bad actors into a digital playground for monitoring.
DECOYnet	Emulates an enterprise's unique IoT systems.
GuardiCore	Redirection architecture and dynamically generated live environments engages attackers and identifies their methods without disrupting data center performance.
MazeRunner	Realistic environments to attract and hunt cyber attackers.
Novo	Active user behavioral analytics software that combines machine learning and decoy technology.
TrapX	Deceives would-be attackers with turnkey decoys (traps) that "imitate" your true assets.
Wire Transfer Guard™	Deception solution built specifically to protect high-value data and messages in wire transfer systems.

The Honeypot Projects

For almost 20-years, honeypot projects have been in existence luring would be attackers to investigate hives full of simulated trophies of compromise. These nonprofit or volunteer projects have made significant contributions to reducing threats to our networks by sharing their results.

These are the top-3 honeypot projects:

- OWASP Distributed Web Honeypot (DWH) Project – Since 2006, the goal of the DWH Project is to identify emerging attacks against web applications and report them to the community including automated scanning activity, probes, as well as targeted attacks against specific web applications.
- Project Honey Pot – Founded in 2004, Project Honey Pot is the first and only distributed system for identifying spammers and the spambots used to scrape addresses from websites. Project Honey Pot has prevented billions of SPAM messages from hitting user email bins.
- The Honeynet Project – Founded in 1999, The Honeynet Project is an international security research organization, dedicated to investigating the latest attacks and developing open source security tools to improve Internet security. The Honeynet Project has contributed to fighting malware and malicious hacking attacks such as the infamous Conficker worm.

If you wish to dip a toe into the honey, start by investigating these projects. See what they have learned and apply those lessons to your own organization gauging whether they would have or could make a difference.

WHAT IS THE VALUE OF A HONEYPOT?

So what do you want to use honeypot data for anyway? Finding harbingers of an attack is one of the principal benefits of deploying a honeypot. Once a hacker revels their intent and approach, you can create a mitigating plan of action.

At a very high-level, you can identify connections by country and block those addresses your organization has no legitimate business interaction.

You can also review the top usernames, passwords and combinations to ensure they do not exist in your enterprise. The real detailed threat intelligence will come from honeypot solutions that allow real attacker interactions.

I also believe you buy precious time by allowing hackers to attack a faux site. Honeypots provide insight into the types of attacks headed your way allowing you to shore up your cyber defenses and create hacker profiles.

Conclusion

Honeypots have stirred a lot of controversy over the years and there are those that would say their time has come and gone. I on the other hand believe their time is at hand. I advocate a hybrid approach or honeypots on steroids where an organization utilizes cyber deception as an intelligence gathering method as part of their overall intelligence tradecraft.

ABOUT THE AUTHOR

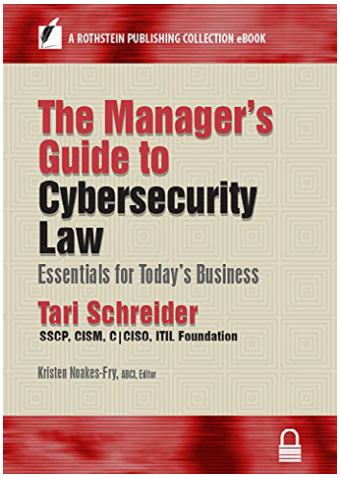
TARI SCHREIDER

C|CISO, CHS-III, CRISC, ITIL™ v3, MBCI, MCRP, SSCP

Chief Cybersecurity Strategist & Author
Prescriptive Risk Solutions, LLC.
Atlanta, GA - Cheyenne, WY

www.prescriptiverisksolutions.com
tari@prescriptiverisksolutions.com

M: Atlanta – 678.595.2818
M: Cheyenne – 307.215.1330



The Manager's Guide to Cybersecurity Law

Qualifies for Five (5) EC-Council ECUs.