Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Honeypots

Prof. Dr. Bruce Nikkel

Ancient History

Sun Tzu, The Art of War, 500BC (v. Chr.)

All warfare is based on deception, Chapter 1

- when we are able to attack, we must seem unable
- when using our forces, we must appear inactive
- when we are near, we must make the enemy believe we are far away
- when far away, we must make him believe we are near

Modern Military/Gov Deception

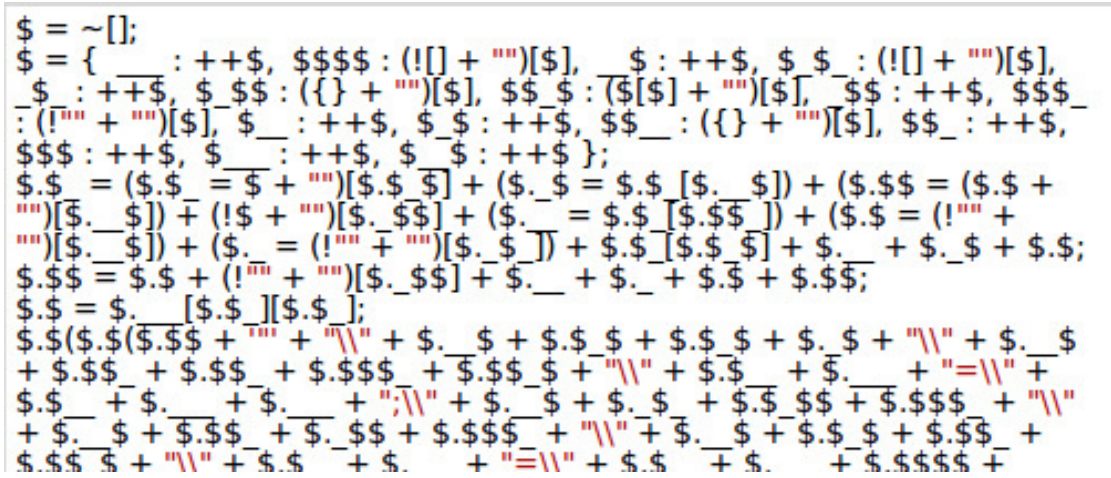
Militaries try deceive the enemy

- fake capability
- hidden capability
- counter intelligence
- manipulate information
- government spy vs spy

From Snowden leaks:
`https://archive.org/details/gchq-online-deception/`

Modern Cyber Deception

Criminals do it all the time



- anonymized IPs
- spoofed packets
- spoofed emails
- phishing websites
- malware - files intended to look harmless
- obfuscation - malicious javascript, polymorphic code

Security people do it a little bit...

- firewalls - hide hosts and ports
- split DNS - hide internal network
- security by obscurity ?!?! (moving ssh to port 2222, srsly?)

Honeypots are also a form of deception

Honeypots

Used in computer security

- detection
- intelligence
- investigation
- research

Deception by good guys (hopefully)

- fake computer systems
- fake networks
- fake services
- fake people
- operate at different OSI layers

High Interaction Honeypot

Intended to give attacker maximum functionality

- vulnerable OS or application
- unpatched, bad configuration
- no security software (firewall, AV)
- functional, real environment (but no real data)

Expected and allowed to be compromised

- can be a VM or physical machine
- directly exposed to the Internet
- monitored closely for attacks
- analyze the attack after its over

Attackers find it and break in

- find it by scanning or Shodan searches
- port scanning the whole Internet is trivial today

Low Interaction Honeypot

Intended to give attacker "perception" of functionality

- looks real, but is only a simulation
- OS network fingerprint is faked
- services are emulated, not real
- useful for automated scanning
- human attackers will quickly learn its fake

Safer more controlled honeypot environment

- installed as a honeypot application (honeyd, kippo)
- can impersonate large range of IPs from single machine
- link layer can answer arp requests for non-existent hosts

Sticky honeypots, or tarpits

- accept connections, but slow them way down, keep them alive
- lebrea - original tarpit daemon (named after a dinosaur park)
- endlessh - slow display of endless ssh banner

Spamtraps - Email Honeypots

For attracting spammers

- post/publish spamtrap email addresses in public forums/lists
- embed email addresses in html (machines see it, people don't)
- when spammers are harvesting addresses, they find your spamtrap address
- email to your spamtrap addresses can be analyzed, monitored
- good for anti-spam, and collecting new malware samples

Honeypot mail servers

- functional DNS, MX records, SMTP daemon
- look like normal servers that accept mail for delivery
- can act like open relays, but quarantine everything
- also good for infected client honeypots sending spam

Client Honeypots

Sometimes called honeybots or malware drones

- client machine is purposely infected with malware
- can be manual infection by malware analyst
- automated infection with client side honeypot farms
- can be virtual machines or physical machines

Used for malware analysis and malware research

- mitm for traffic analysis
- monitor botnet communication
- memory dumps of infected machine
- filesystem forensic analysis

Depending on the malware, may refuse to infect under some criteria (region, machine type, user environment, etc.)

Botnet Sinkholes

Honeypot for a whole botnet

- "fake" Command and Control (C&C or C2) server
- taking control of botnet's C2 server or DNS domain
- DGA (Domain Generation Algorithm) predicted, future DNS domain(s) registered in advance
- all infected bots connect to sinkhole server

Botnet herder (owner) loses control

- part of police assisted action (siezed domain or server)
- security researchers finding vulnerabilities in botnet
- can also be criminals steeling control from other criminals

abuse.ch and shadowserver.org are good resources

Internal Routing/DNS Sinkholes

Sinkhole servers, honeypots for internal infrastructure security

- organizations must use strict proxy access to Internet
- no NAT or routed traffic, everything configured via proxies
- no DNS resolution for external names, all via proxies
- internal default route sends external traffic to sinkhole
- internal DNS queries for external domains resolve to sinkhole

All internal PCs attempting non-proxy external connections or DNS resolution are suspicious

- no false positives, all sinkhole hits are attempts to bypass proxy
- can detect malware in the process of infection (direct attempts to fetch loaders, contact botnet C2)
- detect rogue software installations and misconfigured machines
- detect attempted data exfiltration, covert tunnelling

Honeynets

Honeypots can be managed in groups of machines or IPs

- called honeynets or honeypot farms
- can be client or server honeypots
- can be distributed across many ISPs/Hosters around the world
- can be on a single large range of IP addresses

For single large IP range

- single honeypot machine can simulate entire IP range
- useful for passive listening for Internet scanning activity

For globally distributed honeypots

- have a better view of Internet, not geo-fenced
- observe regional targeted scanning

Honey Links

Web links that are visible to machines but not people

- can be embedded in html pages, single transparent pixel
- crawlers find it, humans don't

Robots exclusion standard

- made to instruct visiting search engines
- ROBOTS.txt file lists forbidden directories
- special directories (honey links) can trigger response
- attackers, pentesting tools, and nasty search engines will find them, visit them

Website Tracking (fyi, use Privacy Badger, ad blockers)

- 3rd party tracking bugs
- social media "share" icons are spying on visitors
- analytics sites gather info, match with past cookie data

Tracking Bug Honeypots

Link usually sent via email

- also called webbugs or beacons
- used by advertising and marketing companies
- used by spammers, and criminals to distribute malware
- can be used by investigators and researchers

Web links are embedded in html mail or documents

- when opened, the client visits a honeypot
- fetches a single pixel transparent gif
- not visible to user, but honeypot server gets information about IP, browser/client, OS, etc.
- can trigger additional information gathering

Not limited to html images, can also be DNS, reverse-DNS, calendar invites, other application protocols

Exit Node Honeypots

Anonymization

- TOR (The Onion Router) - cryptographic system for anonymizing network traffic
- anonymizers and relays are dedicated servers (or tiers of servers) to mask IP source addresses
- designed to hide the identity of the originating machine at the network layer
- but not anonymizing the upper layers (session, application)

These services have exit nodes connecting to final destination

- anyone can create a relay or an exit node honeypot
- including criminals, researchers, other agencies
- original IP is gone, but the rest of the traffic can be analyzed or manipulated
- more interesting in the days when nobody used encryption

Other Honeypots

Honey phones or honey mobiles

- infecting phones with mobile malware, rogue apps
- make/accept voice calls, SMS messages
- social engineering

Honey docs

- specially prepared documents for attacker to find
- contain false or deceptive information
- contain malware or other malicious content

Honey people

- fake user acccounts
- social media profiles (linkedin, facebook)
- get access to contacts, content, communities

Legal Risks with Honeypots

What if somebody uses your honeypot to commit a serious crime?

- are you an accomplice to criminals who use your honeypot?
- maybe the attacker is spamming, or participating in a DDOS attack, but what if the damage is more severe?
- child exploitation, unauthorized ebanking access to steal money, or a terrorist communication channel?
- You can't say you were not aware, you built it fully expecting to have nasty people attacking it!

Which jurisdictions are involved? That is important!

- the country where you are
- the country where your honeypot is hosted
- the country where relayed attacks are targeting people

Depending on the crime and jurisdiction, an international legal process may be started

Any Questions?

Any Questions?

Thanks for listening!

Contact: bruce.nikkel@bfh.ch