



HONEYPOINT Security Server

Supported Operating Systems

- Windows, Linux (with GTK2), OS X, VMWare & other virtualization solutions

COMPONENTS

Console

- Runs as a GUI application
- Role-based access controls built in
- If console is offline, HPoints cache event data to disk, report when back online
- Features automatic enrollment of HPoints to minimize management resources

HPoints

- Traditional HoneyPoint behavior - listen for incoming connections, emulate services, capture and report transactions
- HornetPoint “Defensive Fuzzing” behavior - listen for incoming connections, emulate services, fuzz expected responses, crash connecting malware/clients, capture and report transactions
- Runs as a service in Windows and/or daemon in Linux/OS X
- One binary deployed for each port dilated in current version (changing soon)
- Little to no impact on processor/memory
- Designed to be run on existing servers and workstations
- No signature updates, “deploy and forget”(SM) architecture
- No false positives, all events are suspicious at best, malicious at worst

Trojans

- Small binary or HTML files that can be placed around the environment
- When opened/executed, they make a call to a HoneyPoint, revealing source and data about the offending system
- Can be used to track a piece of data as it moves around the world
- Creates the basis for a Corporate Counter-Intelligence (CCI) program
- Custom compiled per customer, each with its own MD5 & SHA-1 hash to prevent easy detection by attackers

Decoy Hosts

- Virtual machines based on small, hardened Linux installs
- Host various HPoints
- Deployed in virtual environments with multiple virtual interfaces across VLANs, etc.

HPSS Proxy

- Licensed separately
- Runs as a service/daemon
- HPoints deployed in a segment (DMZ) or a remote network can be configured to use this as a console and it forwards data to the real console
- Allows simplified ACL and port exposures on routers and firewalls

Alerting Capabilities	<ul style="list-style-type: none"> •Email/Paging/SMS •Event log in Windows, Syslog in Linux/OS X (SIM/SEIM integration) •Plugin interface (see below) allows custom alerting methods and actions
Reporting Capabilities	<ul style="list-style-type: none"> •9 built in configurable HTML reports •Print to PDF if the OS supports it or with 3rd party applications •Database is SQLite so custom reports are easy to create with various commercial and open source applications
Plugin Architecture	<ul style="list-style-type: none"> •Custom meta-language allows users to trivially extend the product •Design/integrate with custom applications •Perform/automate various responses (update ACL's, .htaccess, scan back, etc.) •Users can choose any license type desired for each plugin and underlying code •Plugins may be licensed separately, as users create them
Emulated Services	<ul style="list-style-type: none"> •Web server (HTTP), SMTP, POP3 •Cisco style 2 level login TCP service (example: banner with password request) •Traditional style (ftp, etc.) 3 level login TCP service (banner, login, password) •TCP & UDP non-responsive listeners •Port mining listeners (TCP listen with send large binary file to crash malware) •Various and custom services available and released often
Communications Strategy and Cryptography	<ul style="list-style-type: none"> •HPoints only interact with Console during events to prevent detection and minimize traffic •All communications are 128 bit Blowfish encrypted •Protocol is a customized encoded protocol that prevents replay
Event Metrics (on average)	<ul style="list-style-type: none"> •Typical Internet exposed HPoints receive 3-5 events per day, per HPoint depending on emulated service •Typical internal network deployments (500 PCs) receive 3-5 events per month, depending on emulated service and level of additional malware protections in place
Black Hole Strategy	<p>Many organizations use the application to identify probing/scanning addresses on the public Internet and then leverage plugins to update firewall/router ACLs. This can be used to create a "one strike and you are out" defensive posture. When combined with HornetPoint deployments and port mining , this can create a significant malware defense.</p>