

PERSONAL EDITION

HONEYPOINT™

Highly Effective:

Capable of identifying sources of attacker probes, malware, scanning and other malicious activity

Know when YOU are a target

“Defensive Fuzzing” power of HornetPoints and plugins enable automatic defenses against hackers and their tools

Ultra-Configurable:

Emulates Thousands of System Services and back doors

Both TCP and UDP HoneyPoints

TCP HornetPoints

Cross Platform:

Windows, Linux, Mac OS X and Virtualized host platforms supported



Attackers Target Users, But Now They Can Fight Back!

Users are among the favorite victims of attackers. Their workstations are open invitations for worms, probes and scans as attackers seek every advantage to gain control over the network.

Attackers will stop at nothing to gain control and one of their favorite tactics is to leverage user workstations, passwords and access. Compromised while on the road at coffee shops, hotels and airports or through social engineering attacks via email, attackers have developed powerful tools called “bots” to help them in their quest.

These bots turn compromised machines into zombies that do the bidding of attackers, even when the machine returns inside your protected networks. As such, users need real-time capabilities to know when they are being targeted, scanned and probed. Admins need HoneyPoint technology to help them trace, analyze and mitigate threats as they emerge on the network.

Enter HoneyPoint Personal Edition (HPPE). Based upon our industry leading honeypot technology, HPPE gives users a security solution that is easy to use,

ultra-configurable and highly effective. Unlike firewalls, users can actually see when attackers are targeting their machine, encouraging them to move on to safer locales or take defensive actions.

HPPE intercepts attacker activity in the targeting stage and gives you the capability to quickly understand their source and intent.

*Try it today for **FREE**, then purchase a license at the online store when you are ready.* With HoneyPoint Personal Edition, attackers get stung instead of you!

How Fake Applications Can Make You Safer

How can something that's not real add to your security? Easy, if you understand the power of HoneyPoint. When your computer serves up applications that aren't real, then there is no reason for anyone to interact with them, ever. Any interaction with them, at all, can be considered suspicious at best and malicious at worst.

Attackers pick their targets based upon the availability of services. They scan or probe all of the devices on the network looking for the ones that might be exploitable with their tools. Malware, bots and worms simply automate this process. They systematically scan network addresses for victims, spreading their malicious payload as they go.

Now, with HPPE, you can turn the tide on hackers, data thieves and malware. You can "catch them in the act", while they are performing their targeting sweeps and often before any damage is done. HPPE alerts you whenever someone, or something, communicates with the fake services and reports their source address and exactly what they did, what data they sent and when the probe occurred. Plugins and HornetPoint functions can also extend the system to create automated responses, custom alerting or defensive reactions when the system is threatened.



"Customers often talk about how they have used Honey-Point Personal Edition to identify when their laptops were being messed with at coffee shops, airports and hotels. They continually praise how HPPE gives them real insight into the threats they face when they are out and about.

It has a strong history of success and works well with their personal firewalls to drive home the idea that it's time to move on when bad things happen!"

-Constance Matthews

Users can decide when they should move to higher ground (or another coffee shop) or when they need to notify their security team if they are on your corporate network. HPPE gives them security vision and real-time feedback on their threats and helps them learn to make safer, more secure decisions.

For technical users and administrators, HPPE gives the the ability to create "drop in" security sensors on the network and to monitor the corporate environment for worms, bots, scans and other insider/illicit behaviors. Many adminis-

trators move the product from system to system frequently, searching for the signs of security compromises and attacks. Since there are no false positives and no signatures to update, they can get this extra level of security without the overhead of other solutions.

That's how fake applications can make you and your organization more secure. They can alert you when you are a target, no matter if you are at home, the office or on the road. ***With Honey-Point on the job, attackers just can't believe what they see!***

Technical Details:

Supported Operating Systems:

- Windows
- Mac OS X
- Linux

Emulated Services/Listeners:

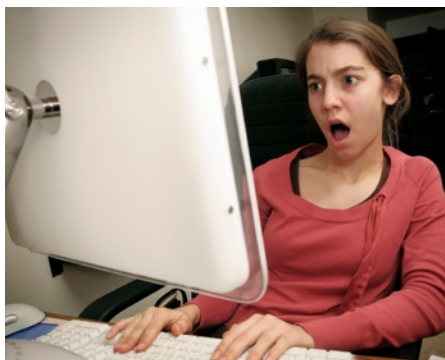
- HTTP/Web server
- Simple TCP service (back door, etc.)
- UDP listener

Runs on hosts in VMWare , Xen, Parallels, etc.

Great for security researchers, technical security analysis and threat monitoring

- Use inside the network for workstations, portables, road warriors and insider threat detection
- Expose to the Internet for ongoing real-time insight into spreading malware, scanning tools, 0-day vulnerabilities and other threats
- Deploy on partner networks or new locations to "quick check" for ongoing scanning, worms, bots and malicious traffic

Give users real-time feedback to help them make better security decisions!



Know When YOU Are The Target

HPPE lets you catch attackers and malware "in the act". You can detect their malicious activity even as they "recon" you as a victim!