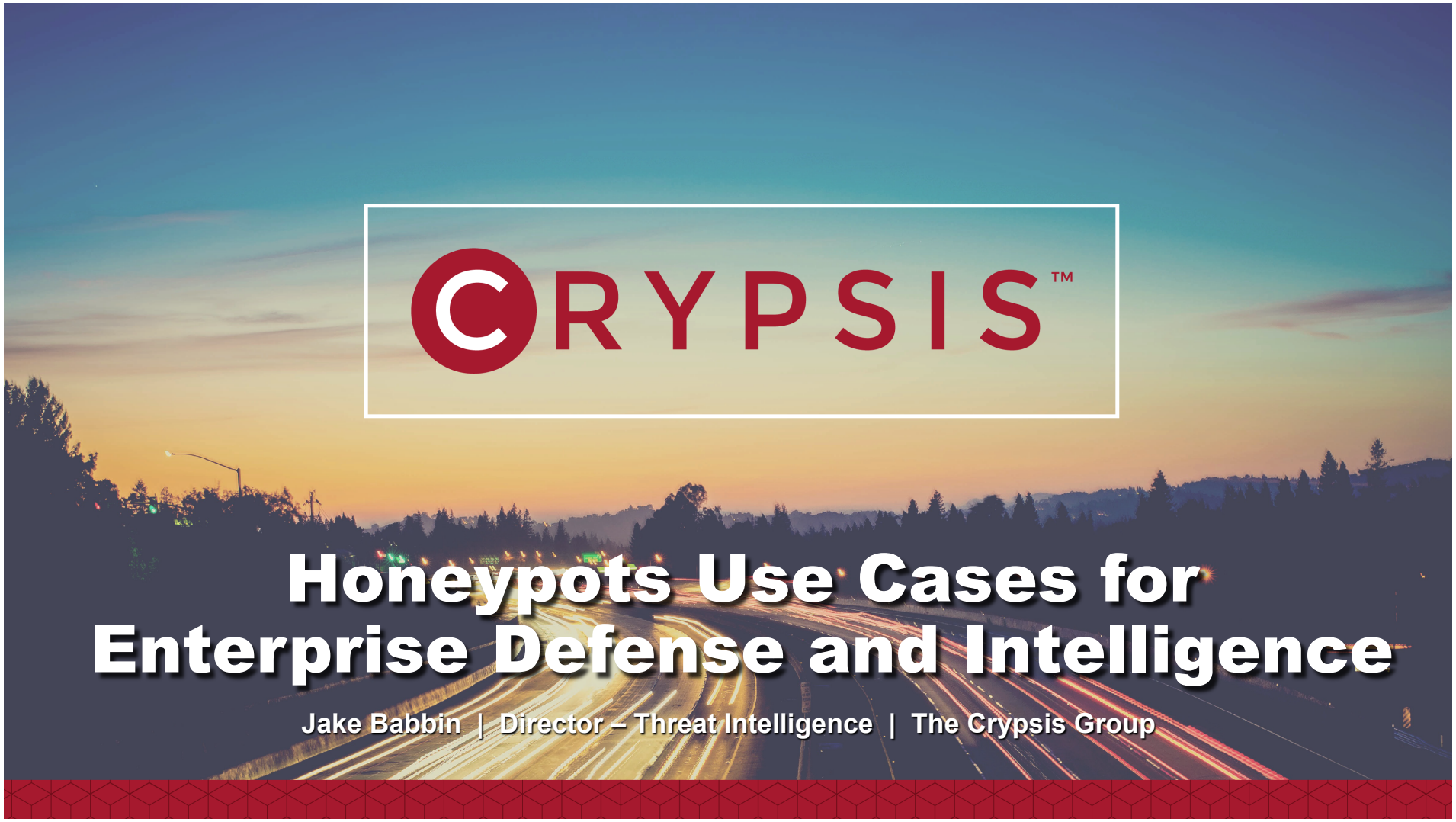

CRYPSIS™
Honeypots Use Cases for Enterprise Defense and Intelligence
Jake Babbin | Director – Threat Intelligence | The Crypsis Group

Agenda

- Speaker Background
- Introduction to Honeypots
- Creating Actionable Intelligence
- Offensive Defense — Taking the Fight to the Bad Guys
- Putting it All Together
- Conclusion

Speaker Background

Currently

- Director of Threat Intelligence, The Crypsis Group

Prior

- Practice Director – Incident Response and Forensics McAfee/ Intel Security (Americas)
- Incident Response Auditor for DoD CIO CND-SP/CCRI team
- Lead Analyst The White House Security Operation Center (EOP)
- Founded The White House Cyber Threat Cell
- Published Author
- Holder of a National Security Trademark
- Over 15 year career spanning a variety of customers in US Military, Intelligence Community, and Federal Law Enforcement

HoneyPot — What Is that?

Honeypot 101

What is a Honeypot?

- An information system resource which has no production values
  - → Its value lies in unauthorized or illicit use of that resource
  - → Its value lies in being probed, attacked, or compromised
    - Lance Spitzer – The Honeynet Project

Honeypot 101

What are Honeypots used for?

- Normally they serve 1 of 2 types of purpose
  - → Intelligence Gathering/Early Warning
    - Attacker Monitoring (TTPs — Tools, Tactics, Processes)
    - Early Warning throughout an enterprise
  - → Bait/Decoy Solutions
    - Placed within Key target location (DMZ, unused network segments, etc.)
    - Support of Incident Response and containment methods

Word of the Day

Honeynet(s)

"A collection of Honeypots that have a centralized management or at least networked together."

Types of Honeypots

Low Interaction
Generally emulate vulnerabilities rather than presenting real vulnerable systems and therefore the attacker is not able to interact with it on all levels.

Medium Interaction (Services)
Similar to a Low Interaction basis with extended protocol/ service emulation. For example might more fully implement the HTTP protocol to emulate a well-known vendor's implementation, such as Apache.

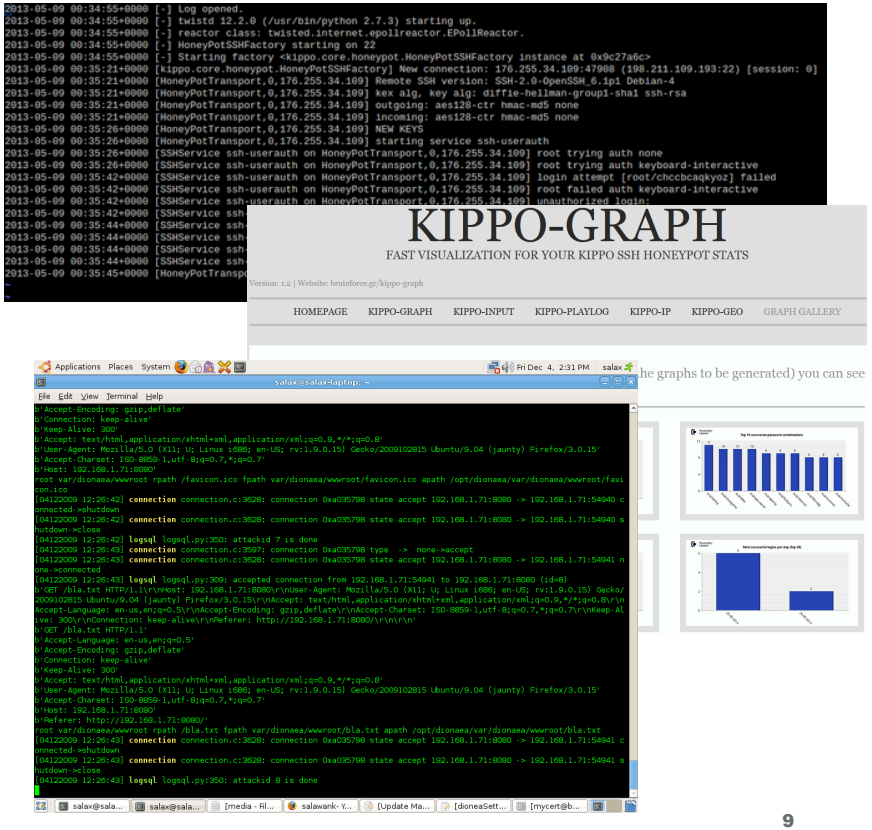
High Interaction (Client)
High Interaction, lets the hacker interact with the system as they would any regular operating system, with the goal of capturing the maximum amount of information on the attacker's techniques, tools and procedures (TTP's).

Low Interaction Honeypots

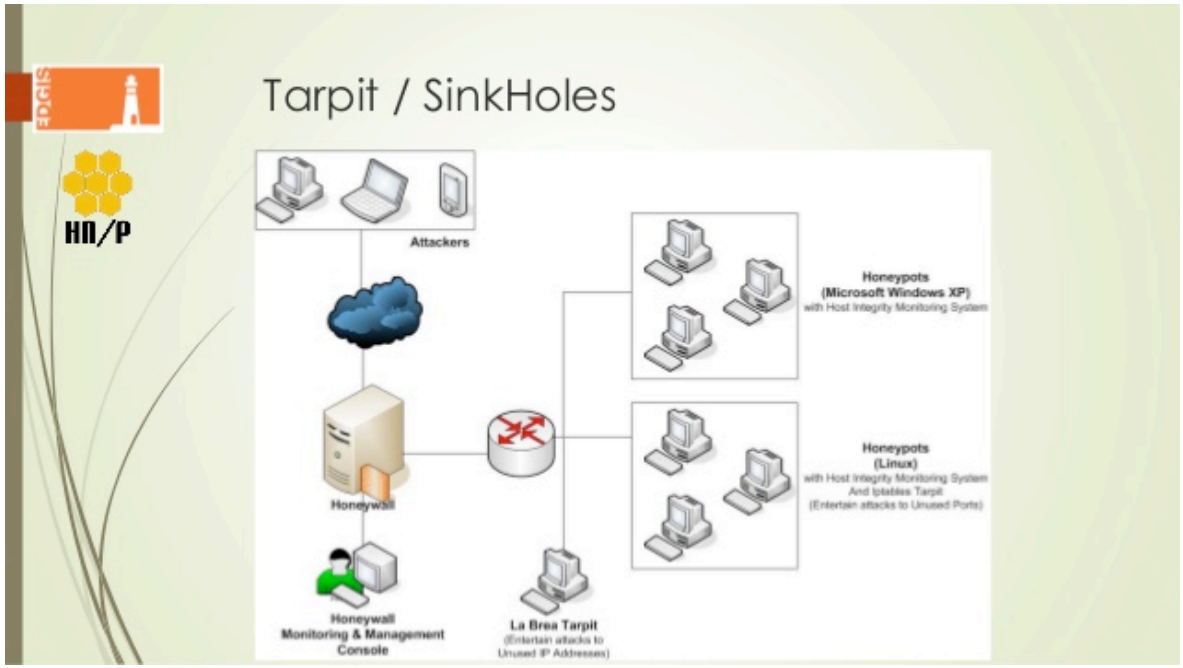
- Often Command Line only
- Quick and Easy to setup

Examples:

- Kippo
  - →Specific Service Interaction
  - →Collects SSH (22/tcp) connections
  - →Add-on can visualize (Kippo-graph)
- Nepenthes/Dionaea
  - →Multiple Service Interactions
  - →Can be High Interaction as well
- Cowrie
  - →Rewrite and extension of Kippo
- HoneyTrap
  - →Focus on Malware collection
- Mailoney
  - →Mail server mimic

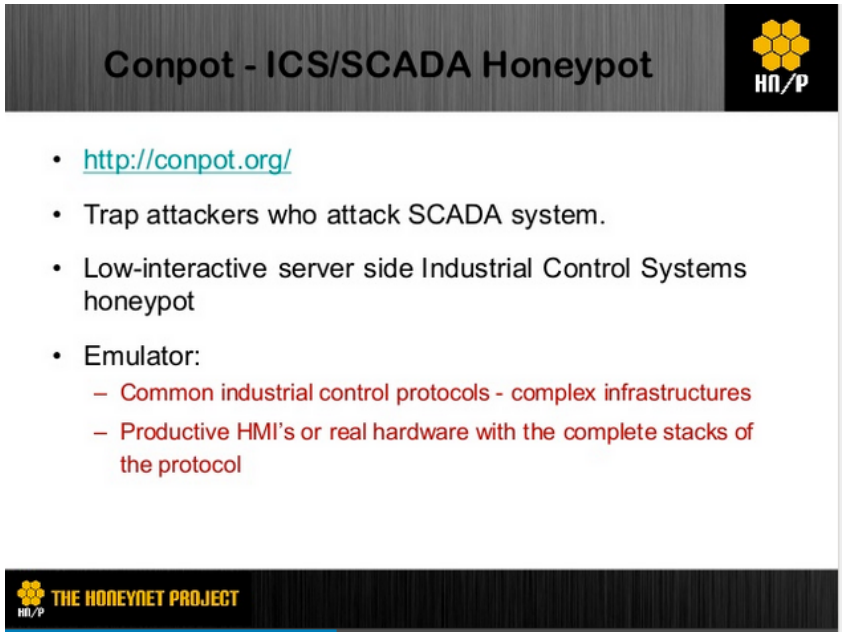


Specific Example — Tarpit and Sinkhole Used for Mitigation and Early Warning System



Taken from Honeynet Project presentation http://www.slideshare.net/efundamental/honeypot-101-slide-share

Specific Type of Honeypot — Industrial Control Systems (ICS/SCADA)



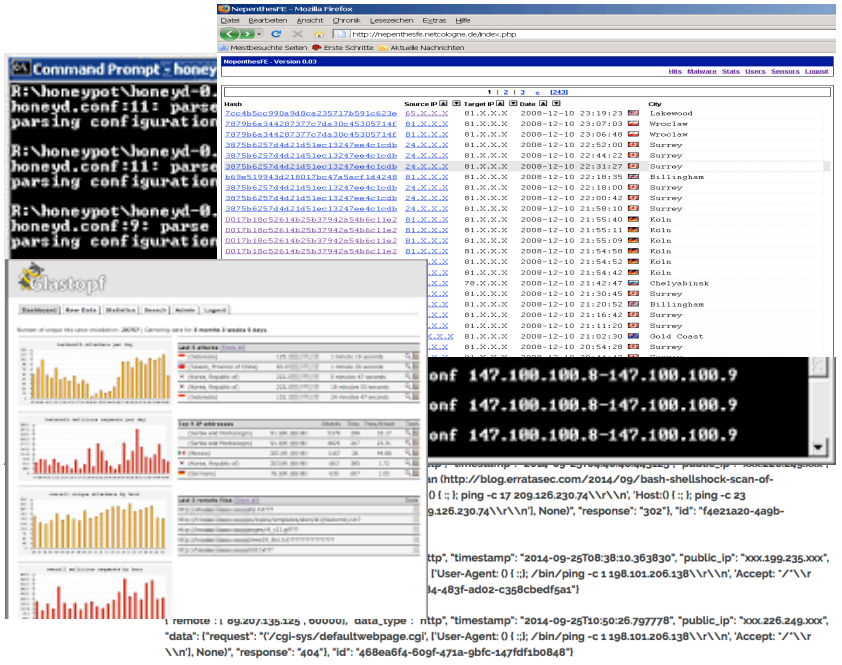
From HoneyCon2016 Presentation http://www.slideshare.net/YuChinCheng/honeycon2016honeypot-updates-for-public

Medium Interaction (Services) Honeypots

- Require specific tuning for proper usage
- Used for specific interactions/captures

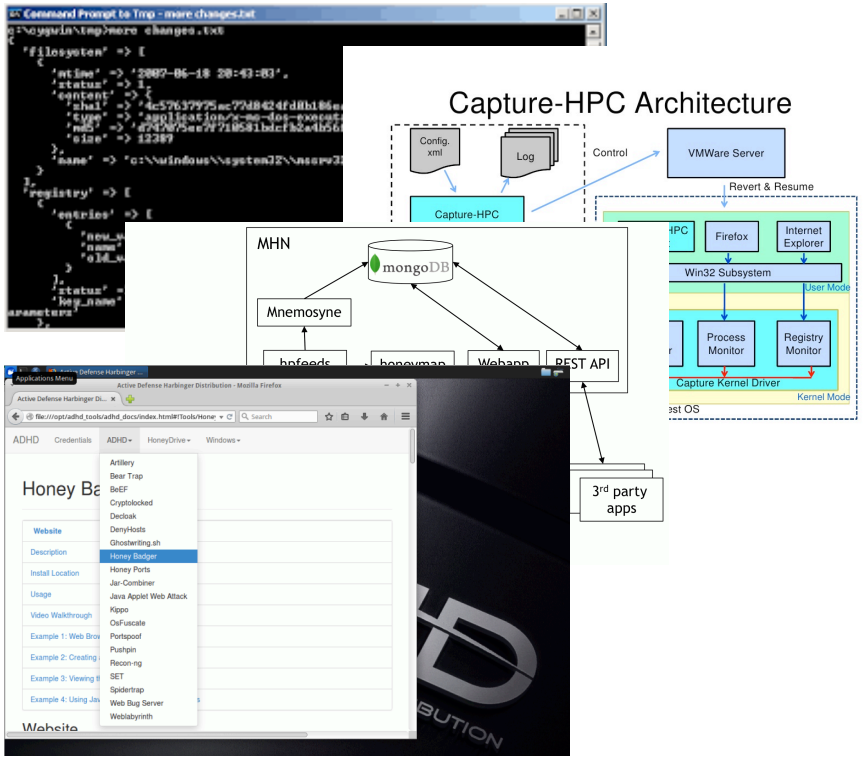
Examples:

- Nepenthes/Dionaea
  - → Malware collection and processing
- Honeyd
  - → Service emulation with scripting
- Glastopf
  - → Web Applications
- For specific detections
  - → Wordpot — Wordpress targeting
  - → Shockpot — Shell Shock (bash) attempts
  - → ElasticHoney — A Simple Elasticsearch Honeypot



High Interaction — (Client)

- Tools
  - → HoneyClient
  - → HoneyMonkey
  - → CaptureHPC
- Platforms
  - → MHN (Modern Honey Network)
  - → ADHA (Active Defense Harbinger Distribution)



You Can Participate as Well at Home!

- HoneyDrive — https://bruteforce.gr/honeydrive
  - → A project out of Greece that combines several honeypot technologies on a single virtual machine environment.
  - → Great for experimentation with solutions prior to deploying in the field.
- ADHD (Active Defense Harbinger Distribution) — https://sourceforge.net/projects/adhd/
  - → Pre-packaged honeypot and attack-back distribution (Ununtu based)
  - → Can be deployed in production
- T-Pot – Tmobile (Germany) — http://dtag-dev-sec.github.io/mediator/feature/2015/03/17/ concept.html
  - → A honeypot platform based on the well-established honeypots glastopf, kippo, honeytrap and dionaea, the network IDS/IPS suricata, elasticsearch-logstash-kibana, ewsposter and some docker magic.

Actionable Intelligence — Logging and Monitoring

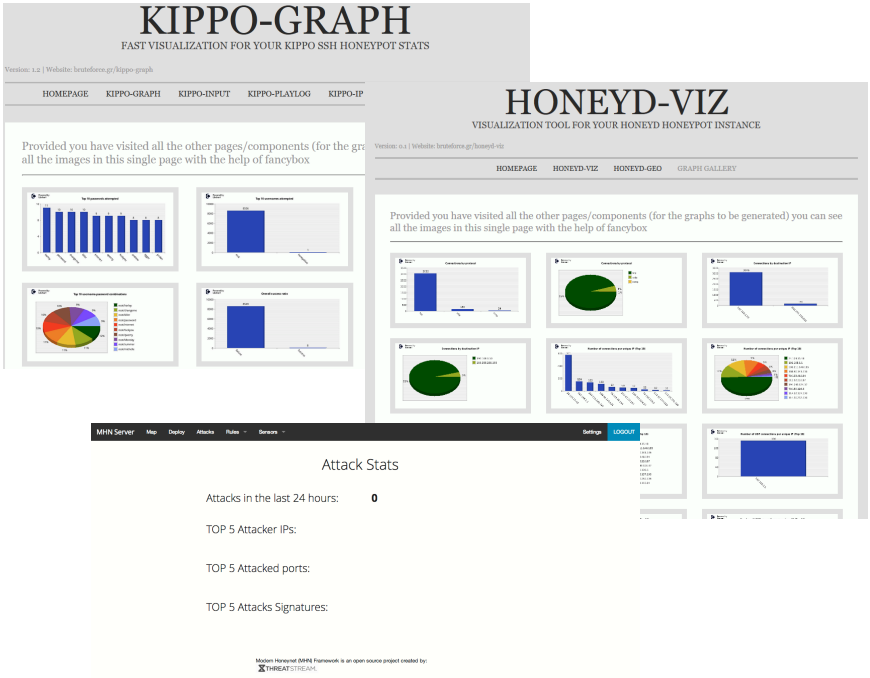
- Early Warning System
  - → Flow/Connection monitoring
  - → Unused IP space access
  - → Web/DMZ access to honeypot
  - → Application Attack on honeypot
  - → Host events (OSSEC/HIPS/HIDS)
- SIEM integration
  - → Active Channels, Watchlists
  - → Correlated events
  - → Filtered Actions
  - → Reporting
  - → NIPS/NIDS signature generation
    - Snort generation

Creating Actionable Intelligence — Honeypot Deployment and Administration

- Deployment Methods
  - → Manual
    - Preparation and obfuscation are Key!
    - Remember Don't Stick out!
  - → Automatic
    - MHN (collector deployment)
    - Scripts
- Honeypot Administration
  - → Kippo-Graph
  - → Nepenthes
  - → Wordpot
  - → MHN – Modern Honey Network

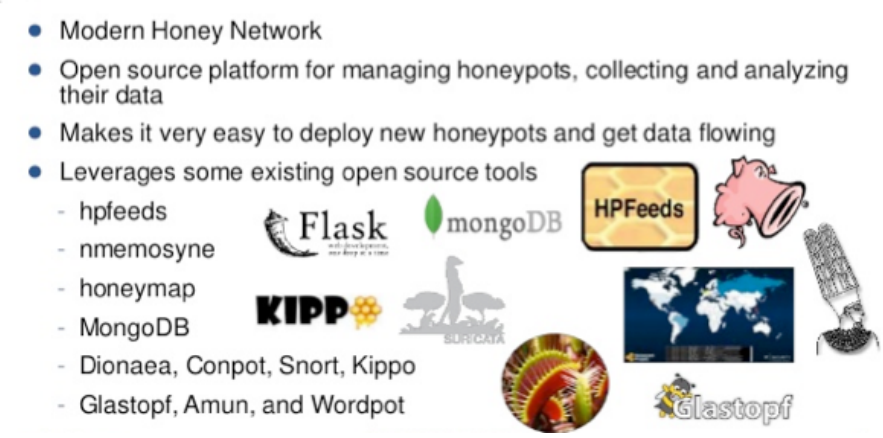
Actionable Intelligence — Visualization

- Platforms
  - → DAVIX
    - Virtual Machine platform with ~50 different tool suites configured
    - See InfoSecCon 2015 presentation by me for lots of examples
  - → Honeyd-viz
    - Web control and frontend for honeyD deployments
  - → Kippo-viz
    - Web frontend for Kippo clients
  - → MHN
    - Provides a light-weight web frontend. Exposure to API's for other tools



Centralized Management and Deployment I've Got a Solution for That!

- One of the difficulties surrounding Honeypot technologies for Enterprise use is managing and collecting data from platforms.
- A solution from Anomali (Open Source!) is called MHN — Modern Honey Network
- An open source system of honeypot management created by the Threat Intelligence company Anomali (formerly ThreatStream).
- "MHN is a enterprise ready honeypot management system which enables organizations to create a fully functional active-defense network in minutes." — Anomali website



Solution: MHN — Modern Honey Network

- MHN is a solution that provides quick deployment and Splunk Integration
  - → Direct management and collection for any deployed honeypot from within Splunk
  - → Script Integration with multiple honeypot technologies
  - → Scripted Deployments for new honeypots
  - → Collection of indicators from honeypot captures
  - → Note: you can also deploy MHN stand alone for custom or specific deployments

Offensive Defense — Taking the Fight to the Bad Guys

- ADHD
  - → Utilize HoneyBadger and other tools to create automatic blocks
- Making the Hits count –
  - → Any IP connecting to a deployed honeypot, create an automatic border ACL block for a set period of time.
    - Great example to shut down scanners, any hit in a honeypot gets added to the border firewall with a block of 30 minutes before being removed again.
    - Breaks the timeout for scanners, but allows for misconfigured hosts to maintain network access after a short break
  - → DNS Poisoning/Sinkholes
    - For malware collection any captured malware, extract the Command and Control (C2) DNS name and add to DNS Poison list for the enterprise. Then any hits in the DNS Poison triggers a SIEM event to detect infections.
  - → Malware submission
    - Two fold solution is possible
      - Capture all malware add to local “DAT” file for your $AV vendor to protect your enterprise from your known attackers malware
      - Capture all malware and auto-submit any file from the honeypot(s) to Virustotal, blowing the malwares’ effectiveness as well as providing community information

Putting it All Together

Threat Intelligence

- Honeypot technologies that are deployed in conjunction with enterprise defense provide a strong solution for an organization.
- Combining honeypot information with Data feeds provides context to alert data.
  - → This IP is associated with a botnet – virustotal
  - → This hash matches a known installer – TotalHash
- MHN (2707) has several options to enrich the data
  - → HPFeeds
    - HPFeeds is a lightweight authenticated publish-subscribe protocol that supports arbitrary binary payloads. – http://github.com/rep/hpfeeds
    - Information can be parsed into threat information for redistribution, alerting and reporting
  - → Endpoint Data
    - Virustotal API access can allow for hash and indicator matching for known hostile files
  - → Network data
    - Project Honey Pot (1457) is another Splunk app that allows Splunk users to get indicators from globally deployed honeypots.
- Integration of Snort and Suricata Network Intrusion Detection Systems can be leveraged to create more accurate detection signatures as well.

Putting it All Together

Splunk

- Apps
  - → MHN (2707) has a great Splunk app that visualizes and shows data quite well.
  - → Project Honey Pot — IP reputation (1457) allows Splunk users to get information from the globally deployed Project Honey Pot Honeynet. (wow!)
- Custom Content
  - → Hpfeeds — an information sharing tool that is part of MHN and several other tools.
    - hpfeeds is a lightweight authenticated publish-subscribe protocol that supports arbitrary binary payloads. – http://github.com/rep/hpfeeds
    - Information can be parsed into threat information for redistribution, alerting and reporting
  - → Endpoint Detection using VirusTotal and AV reporting
    - Multiple integrations with Virustotal are available
    - Includes C2 (DNS/IP) as well as hashing for blocks.

Case Study: MHN and Shell Shock

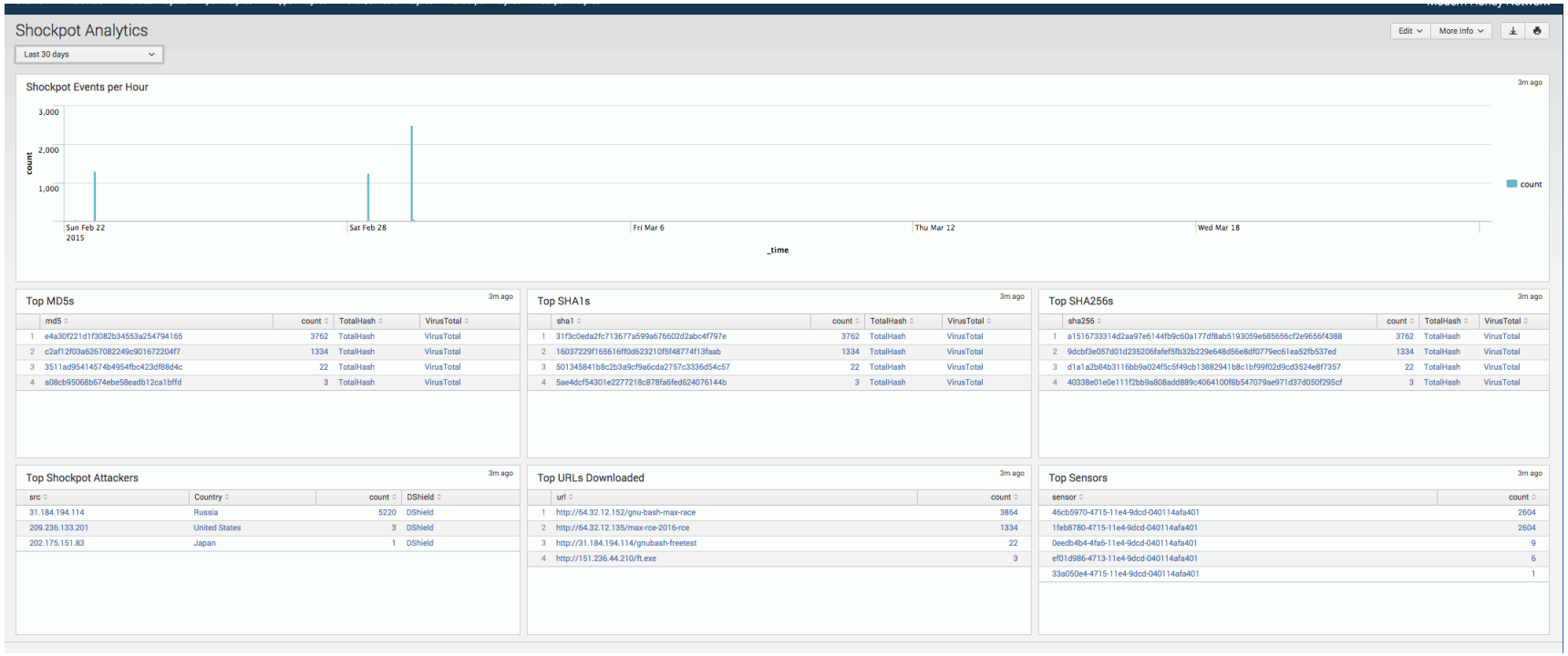
Customer Scenario

- E-Commerce customer is a mixed Operating System environment
  - → Technologies deployed several data centers
  - → Centralized logging via Splunk
- Bash ‘Shell Shock’ vulnerability is discovered and begins propagating. Customer has multiple unpatched machines unknown to them.
- Splunk and MHN to the rescue

Customer Solution

- Leverage Splunk and MHN-splunk
- Deploy MHN for central management
  - → Direct control of deployment and configuration
- Install MHN-Splunk for dashboard content
  - → Provides visibility into exploitation and spread throughout the enterprise
- Deployed multiple ‘Shockpot’ honeypots throughout their enterprise segments.
  - → Specific honeypot example to mimic a vulnerable Shell Shock machine also captures the transmitted malware file(s)
  - → Used internal detections to deploy CIRT responses for mitigations and capture variations in the exploit
- Successfully mitigated, tracked down and patched the affected machines

Example MHN-Splunk — Shockpot Dashboard



Conclusions

Conclusions

- Multiple honeypot technologies that are available to defend enterprise networks
- Integration possibilities with technologies such as Splunk provide immediate Use Cases
  - → Automation and SIEM integration provide enriched
    - Alert actions
    - Reporting
    - Threat integration with data feeds to create Intelligence
- Better allow an enterprise to defend and understand their attackers.
- Provides a flexible and powerful tool in incident response and mitigation strategies.

Thank you!

Questions? Comments?

Jake Babbin – jake.babbin@crypsisgroup.com