Development, Confusion and Exploration of Honeypot Technology

Seak

Antiy Labs

Outline

- Development of Honeypots
- Status Quo of Honeypots
- Technical Challenges
- Exploration and Outlook

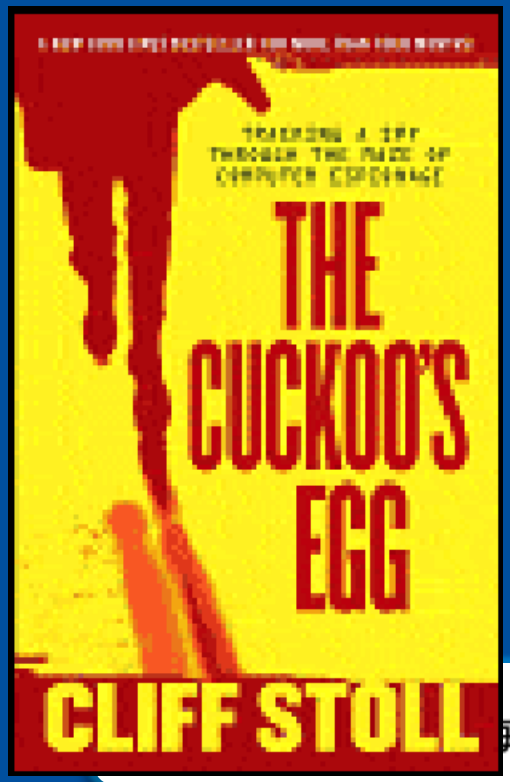
What is a Honeypot?

- A honeypot is a security resource that can be scanned , attacked and compromised.

—Lance Spiztner

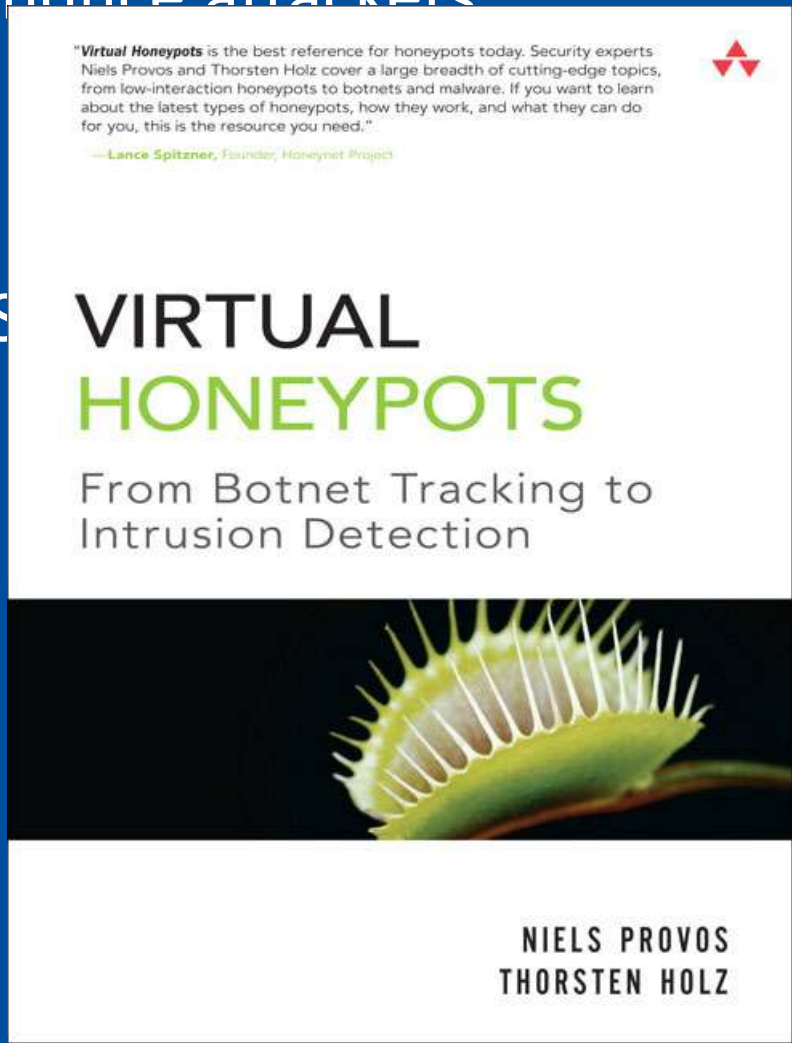
1990-1998: Early Days

- In 1990, *The Cuckoo's Egg* was published.
- Network administrators started using honeypots.
- Physical System



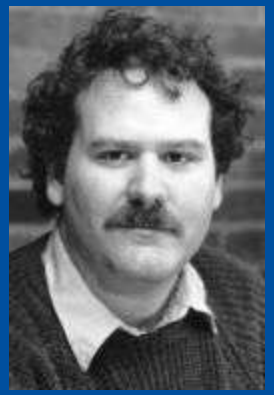
1998-2000: Rapid Development

- Open source tools are used to induce attackers
- DTK（ Fred Cohen ）
- Honeyd （Niels Provos）
- Honeypot products: KFSensor, S
- Virtual Honeypots



Fred Cohen

- The first master in antivirus field
- First used the term “virus”
- Diagonal Method



2000-2006: Prosperous Period

- Since 2000, security researchers tended to use real hosts, operating systems and apps to build honeypots. They also integrated data capture, data analysis and data control systems to security tools.
- main channels to collect samples

Outline

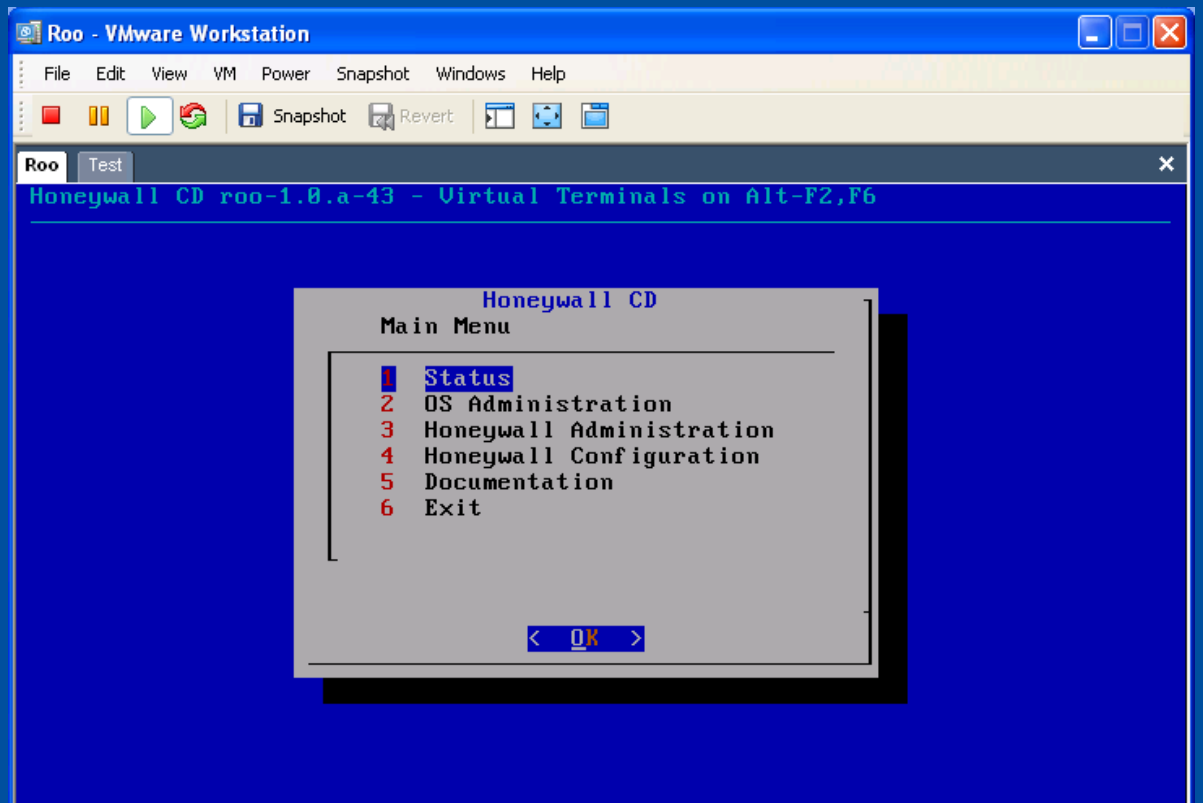
- Development of Honeypots
- Status Quo of Honeypots
- Technical Challenges
- Exploration and Outlook

Categories

- Deploy Purposes
  - Security products
  - Research
- Intensity of Interaction
  - High intensity
  - Low intensity

Honeypots of High Interaction Intensity

- Honeywall CDROM
- Sebek:
- HoneyBow



Honeypots of Low Interaction Intensity

- Nepenthes
- Honeyd:
- Honeytrap:

Honeypot using wireless nodes

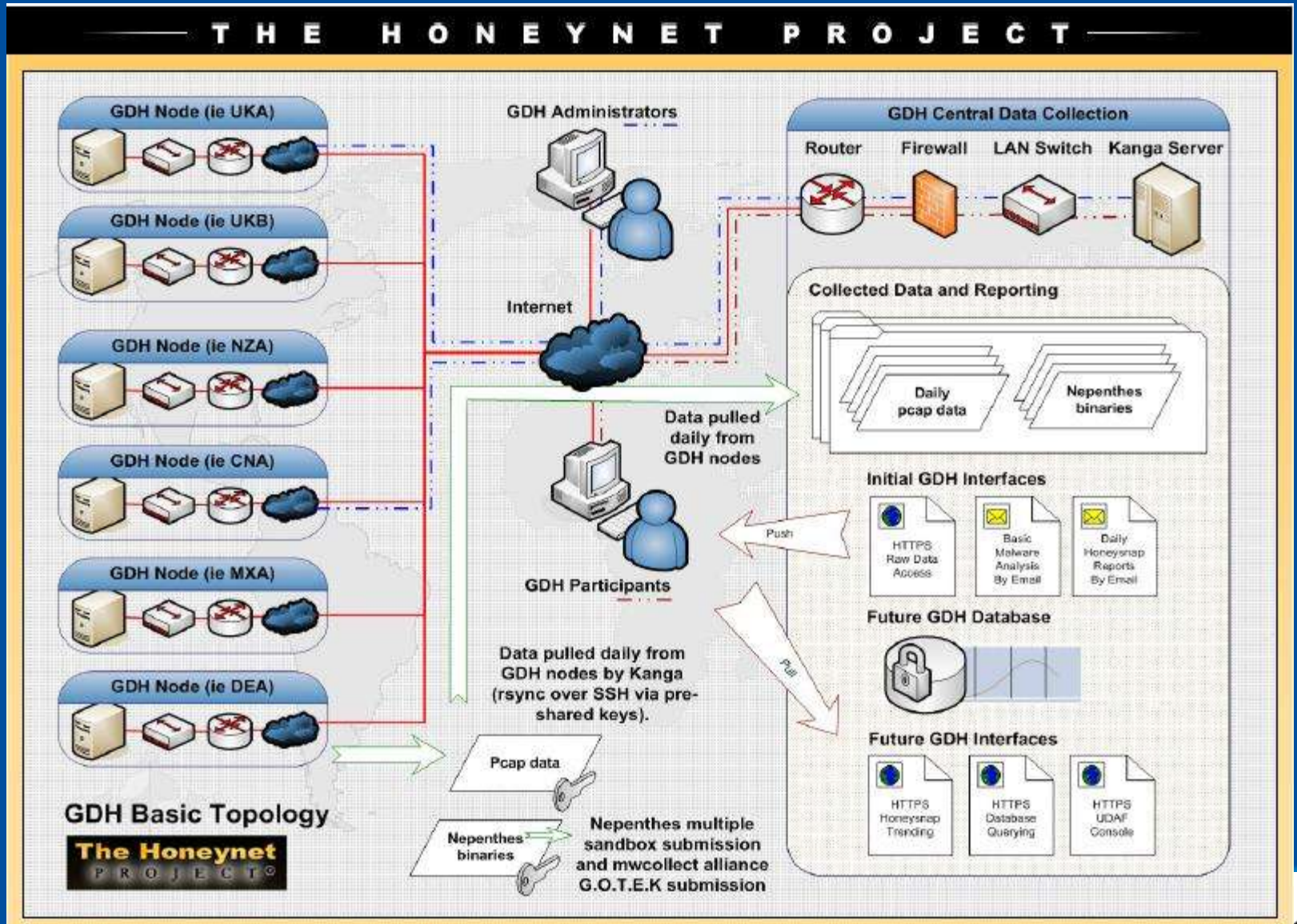
Client Honeypots

- Capture-HPC
- HoneyC

Data Analysis Tool

- Honeysnap

Some Open Source Systems



Some Open Source Systems

Display Filters

Limit: 20

Only data from my sensors:

Magnet Value contains av.clam

+ Add a custom filter.

Filter Binaries

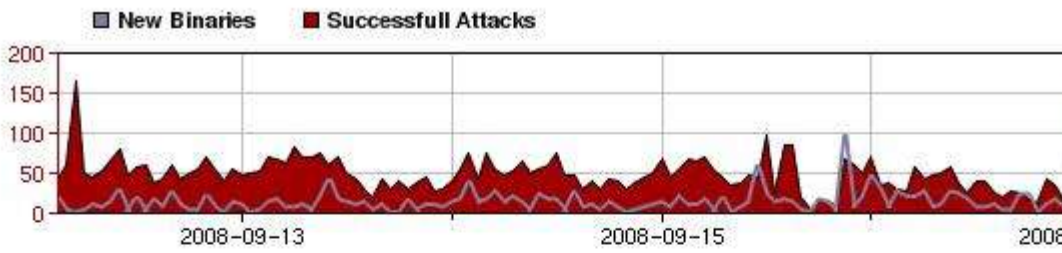
Matching Binaries

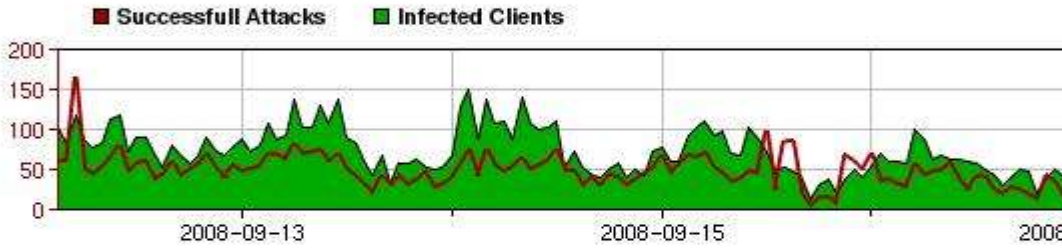
Displaying matching samples 1 - 20.

Hits	Samples	PE Hash
1	1	8e7e49098620ccf78bf6cb05683fcd5c
1	1	?
6	6	bedf4242974d7a0299319722bb5b324b
2	2	ee6d544d4f50628b1bef869ad840e00e
10	10	1c15d334dc0eb44ba335b944f814d1a3
90	90	23162437075ae1ed5d33efc1b167dee7
9	9	ec4461904b376c03389368d5130eaece
52	52	8cb9cb3578438c441f213616a59774b7
158	56	b2cee2a770dd210bd482abd51eb37471
234	234	b45deba4a88553a5f83e27e2fa8a8288
175	175	71d1c85ab3e0782717ffbb4941c16a9c
169	169	19edc87ad51a1beddc2b909716205fb8
489	489	ef2123aebf6cf650d300fb46e773321d
70	70	63ba4ead6d8c8fcbed355b8c411dd2cb
4952	4952	9a32e5f3b0f24a1ca07c4ff0f143c00d
1371	271	169f97a27b1e14ccb44503f82b2acbce
3181	3181	5b8ff0c3cd58c66a451ea102a7a44780
9184	9183	a5afdff73e118584e55de9ed068aad01

«

mwcollect Alliance Activity





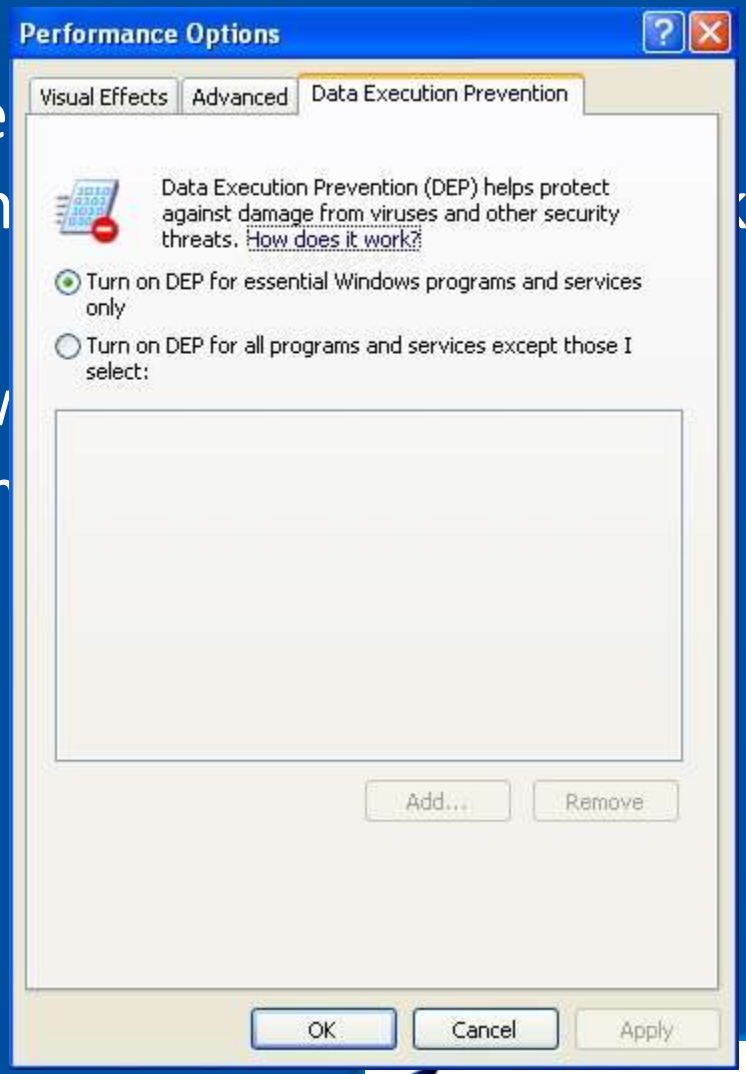
Attack Source Country Distribution

Outline

- Development of Honeypots
- Status Quo of Honeypots
- Technical Challenges
- Exploration and Outlook

Security Threats

- DEP can protect users quite
  hasn't any Windows system
  that can bypass DEP.
- Static format overflow, brov
  based attacks become the r
- The basic working principle
  seriously threatened.



Core Challenges

- Honeypots simulates targets, and then waits for attackers ‘ malicious operations.
- The main attack links are not IP dominated, which makes the situation much more complicated. Attacks are becoming less specifically targeted.

Report All Activities

- Typical report system: OSLoader, drivers, services, processes, modules and IE plug-ins.
- Report large quantities of files + record data frequency + determine as yet unknown malware + automatic analysis system

Representative Distributive Report System

- Eset（NOD32）ThreatSense.Net
- ArrectNET
- Rising “Cloud” Project
- 360safe process report system

Challenges

- Large quantities of desktop security products and clients
- Actual activities
- Zero cost of devices and hardware resources
- Zero cost of distributive computation

Outline

- Development of Honeypots
- Status Quo of Honeypots
- Technical Challenges
- Exploration and Outlook

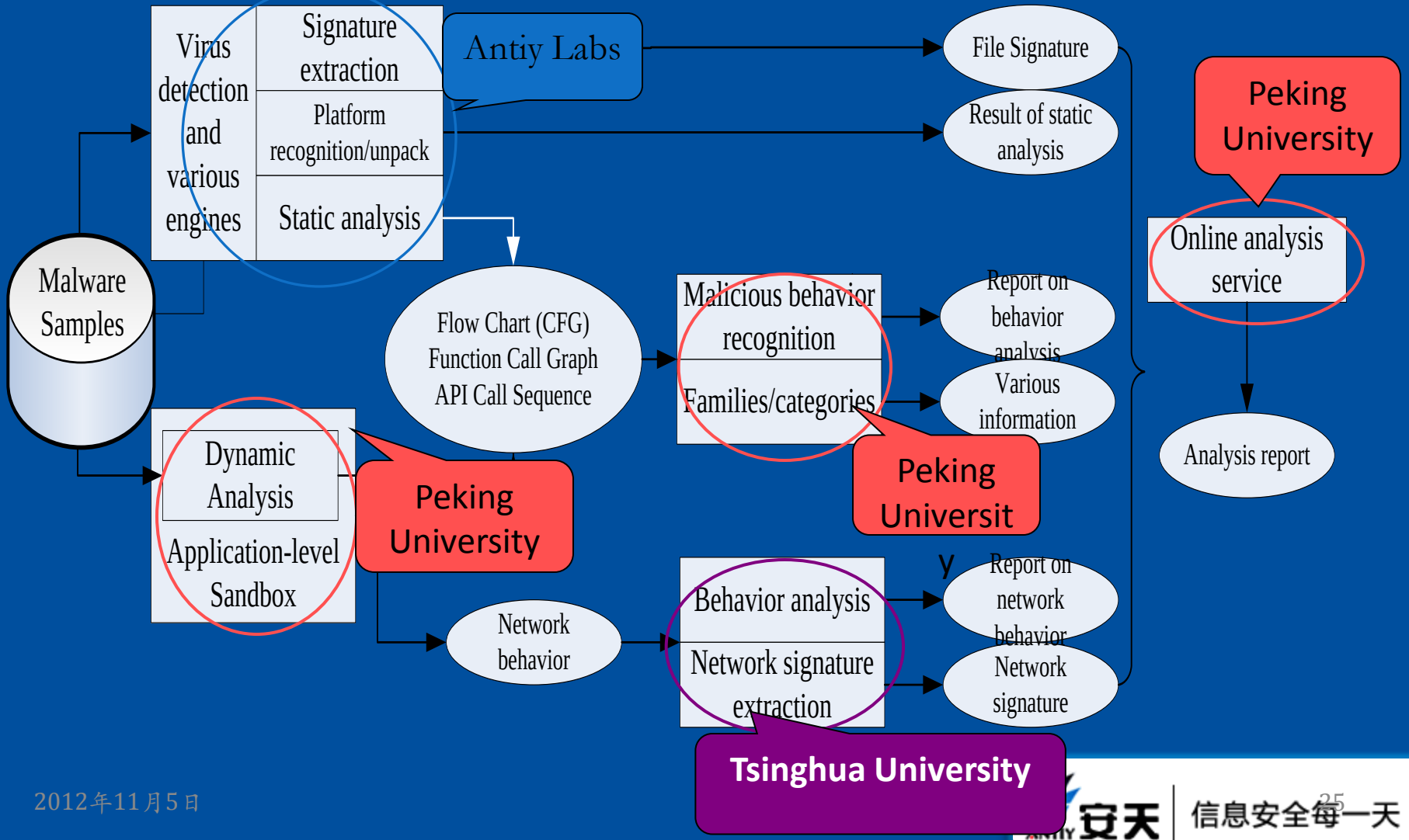
Trend: Sample Cultivation

- Web drive-by download
- Why do we cultivate samples? (incomplete extraction, frequent changes)
- Main sources of sample cultivation

Sample Cultivation and Analysis System

- Research of automatic behavior and signature extraction: Antiy Labs, Peking University, Tsinghua University
- Research of automatic file in large quantities: Antiy Labs, National “863” anti-intrusion and antivirus center, South China Normal University

Research of automatic behavior and signature extraction



Wind-catcher Plan

- Wind-catcher plan: a non-profit honeypot deploy project initiated by Antiy in 2006;
- The plan contains 3 periods:
- Wind-catcher I: improve the national basic capture system
- Wind-catcher II: cooperate with universities
- Wind-catcher III: target at civil researchers and report nodes

Wind-catcher I: ARM Virtual Honeypot

- Demonstration
- Circuit design
- Software system

Telecom-level Honeypot: Honey Pool

Management System

Wind-catcher II: Honeypot Alliance

- Antiy cooperates with Harbin Institute of Technology; Tsinghua University and Wuhan University.
- Deploy 3-5 wind-catcher II honeypots in the universities, share data, and provide basic data for information science research.

Wind-catcher III: ADSL Honeypot

- Small-sized honeypot gateway with dual network cards;
- Can be placed between the use's system and the ADSL Modem

Honeybot

- Security application of NPC;
- Simulate the target value, induce attacks;
- Integrate with traditional system.

Creation in Our Wake

- We appreciate your suggestions.

- seak@antiy.net