PERDIX: A FRAMEWORK FOR REALTIME BEHAVIORAL EVALUATION OF SECURITY THREATS IN CLOUD COMPUTING ENVIRONMENT

botconf

First botnet fighting conference 2013

December 6, 2013

Julien Lavesque – CTO Itrust

j.lavesque@itrust.fr

ITrust
IT SECURITY SERVICES

IKare©
My Business Monitoring in Real Time

- **Security experts company founded in 2007**
- **Historical IT security services department**
  - Pentests, forensic, organizational, training…
- **IKare solution publisher since 2012**
  - Vulnerability assessment and security monitoring solution

- **Security expert for 10 years**
- **Specialized in mobility and Cloud Computing security**
- **ITrust CTO**
- **Pentest department leader**

Context

Traditional security products are no longer efficient against advanced targeted attacks and malwares.

New generation SIEMs include behavior analysis engines to cover these threats.

What about Cloud environment?

- **SIEM products not really adapted to Cloud.**
- **Logs and Flows are not available.**
- **Security controlled by cloud providers**

Conclusion:

To perform **behavior analysis** in Cloud environment, data have to be collected by **external sources**.

Perdix framework

Collect data in the cloud with external scanners…

- **IKare** : the data collector
  - ✓ Vulnerability assessment and security monitoring
    - ○ Discover & identify services
    - ○ Detect vulnerabilities & security misconfigurations
  - ✓ QoS evaluation
    - ○ Services availability & response time
  - ✓ Cloud API
    - ○ Bandwidth usage

> “Targeted attacks, often called APTs, penetrate existing security controls, causing significant business damage. Enterprises need to focus on reducing vulnerabilities and increasing monitoring capabilities to deter or more quickly react to evolving threats.”
>
> Source: Gartner

Perdix framework

… and analyze behaviors

- **Perdix**: the behavior analysis engine
  - ✓ Analysis & learning
    - Statistical analysis & seasonality
    - Learning process
    - Data sources profile
  - ✓ Correlation & Intelligence
    - Reduce false positive results
    - Correlation of different sources analysis
    - Expert system feed
    - Data sample deviation

Practical example – Malware behavior

This example is based on a real malware ran into Perdix framework

- **Malware behavior**:
  - ✓ Based on a known phpBB remote execution code vulnerability
  - ✓ Bot downloaded on remote server
  - ✓ Open IRC server to contact C&C server
  - ✓ Run malicious command
    - ○ Scan all machines to find open shares
    - ○ Try to bruteforce shares access
    - ○ Try to download data
  - ✓ Upload collected data to server

Practical example – analysis

- **Security analysis**:
  - ✓ Based on a known phpBB remote execution code vulnerability

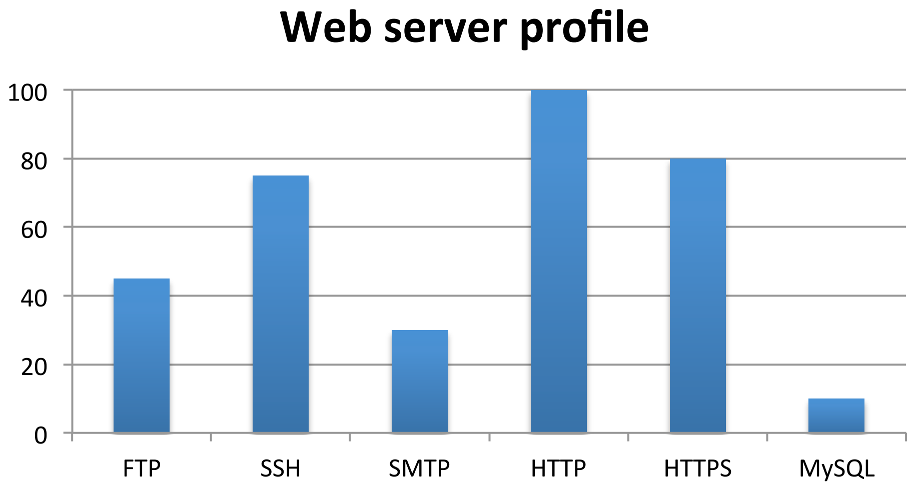
  Vulnerability assessment scan detects the vulnerability

  - ✓ Open IRC server to contact C&C server

  Security scan discovers and identify the service

  The new service differs from the server profile learned by Perdix

  ➢ **The behavior is flagged abnormal.**



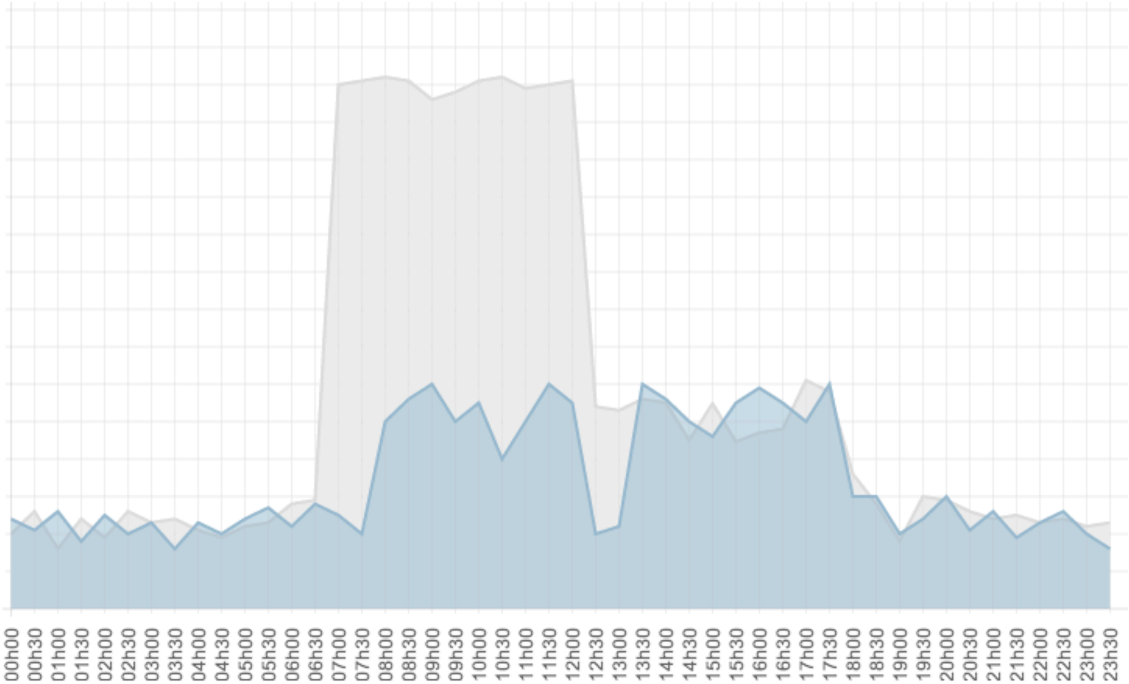
Practical example – analysis

- **QoS analysis**:
  - ✓ Scan all machines to find open shares
  - ✓ Try to bruteforce shares access

The resources used to scan the network and bruteforce access slow down the treatment of legitimate request.

The response time goes out of the threshold from the learned profile.

➢ **The behavior is flagged abnormal.**

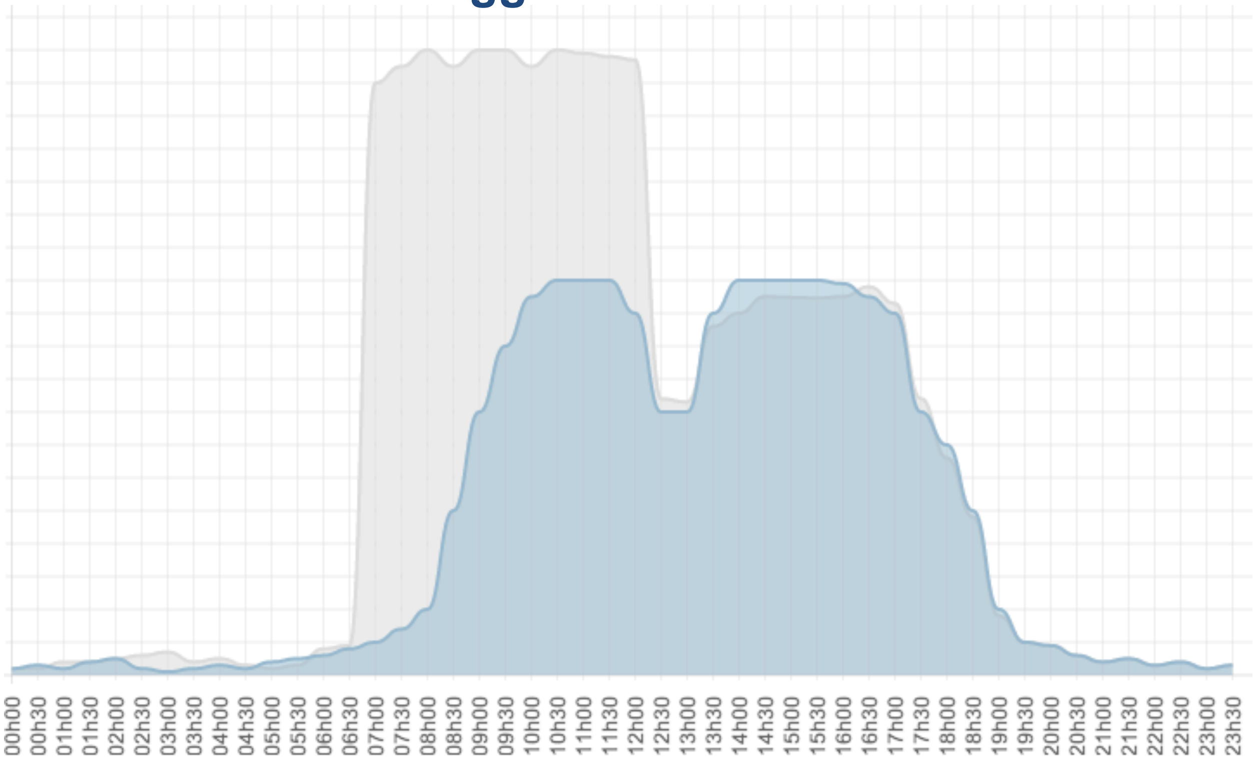


Practical example – analysis

- **Bandwidth analysis**:
  - ✓ Bot downloaded on remote server

  Not significant to raise a flag

  - ✓ Try to download data
  - ✓ Upload collected data to server
  - ➢ **The behavior is flagged abnormal.**



Practical example – alerting

- **Deviant behaviors shall be reported with sufficient information**
  - ✓ Visualize responsible data
  - ✓ Understand elements triggering the alert in natural language

- **Sufficient flags are raised to trigger an alert**

Alert – Abnormal behavior detected – Critical

- Vulnerabilities are detected on the server
- A new service (irc) is detected on the server
- A service (irc) does not correspond to normal behavior
- Server response time is out of normal behavior threshold
- Bandwidth usage exceeds normal behavior

Conclusion

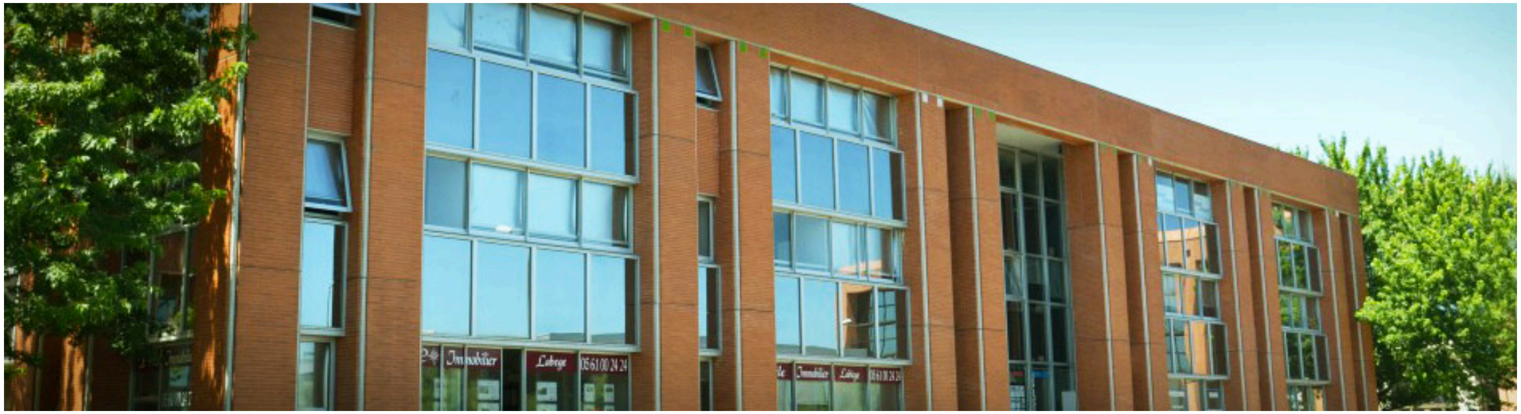
Combination between statistical and learning algorithms provide an efficient tool to detect unknown security issues in a non intrusive manner adapted to Cloud environment.

Preliminary result on the implementation of the Perdix framework on forecasting are promising.

The framework is now tested in a real environment to gather data which are requested for training the behavioral analysis module.

A first version of the framework will be available mid-2014 as it is included in a French government call for projects called **Secured Virtual Cloud**

QUESTIONS ?



ITrust – Head Office
55 Avenue l’Occitane,
BP 67303
31673 Labège Cedex
France

+33 (0)5.67.34.67.80
contact@itrust.fr
www.itrust.fr
www.ikare-monitoring.com