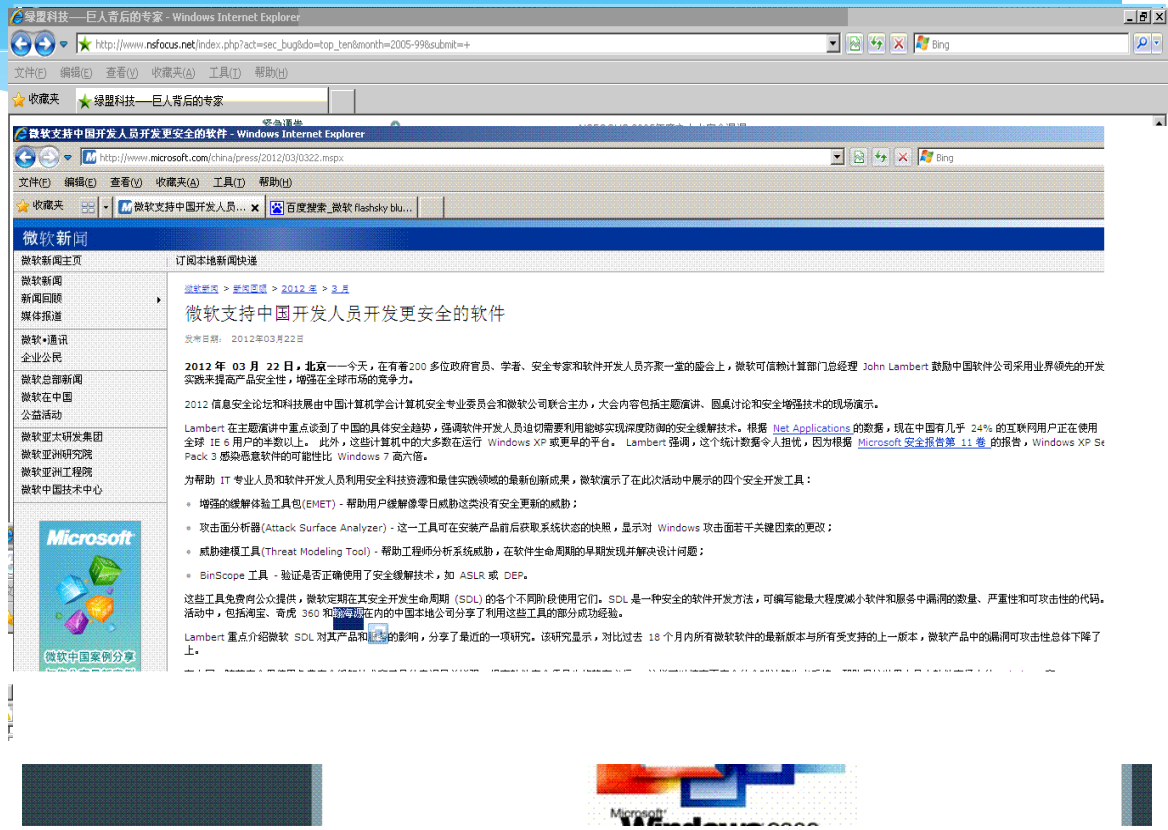
APT Attack Detection of Vulnhunt

Vulnhunt Inc
Flashsky
xing_fang@vulnhunt.com

About Me

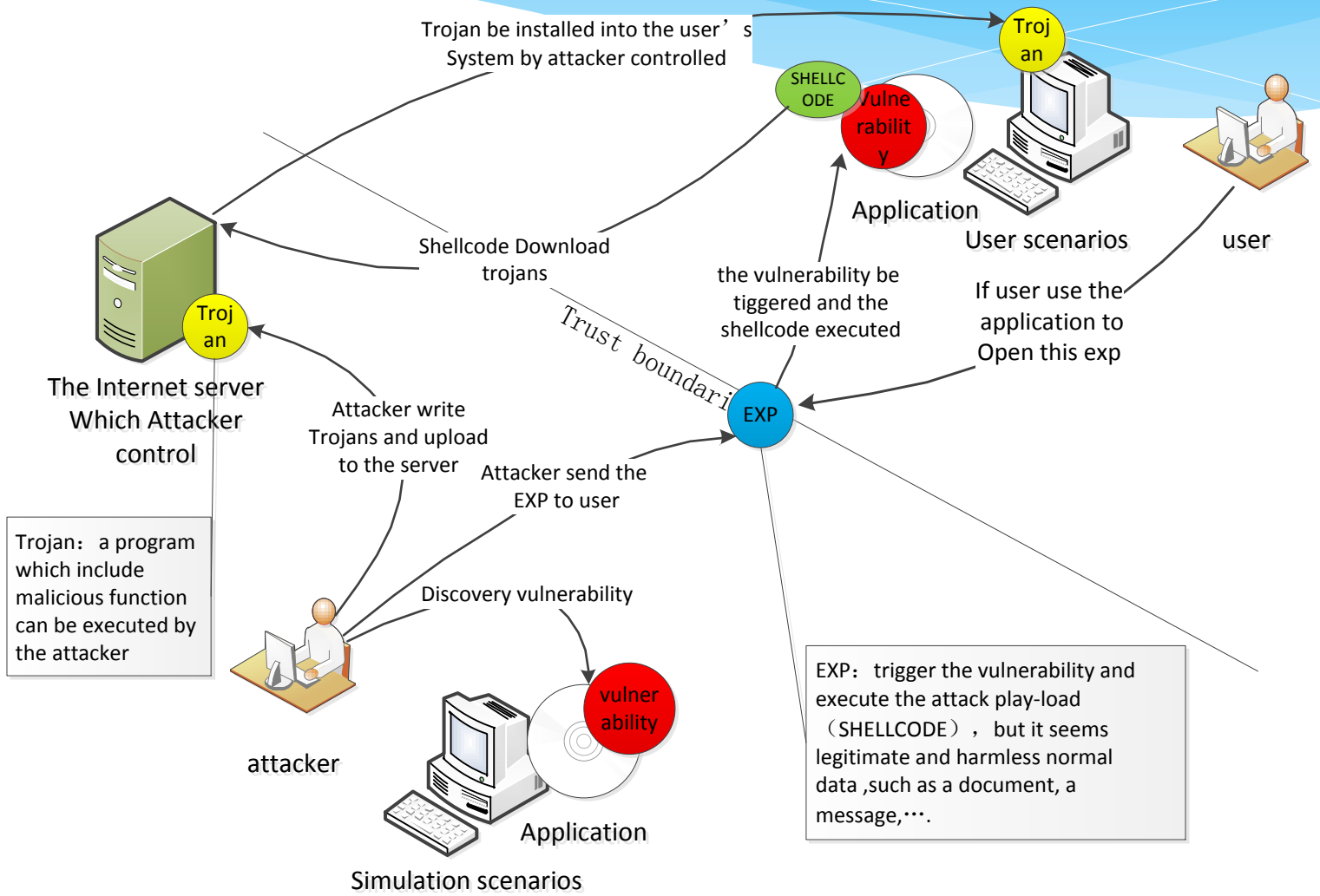
* Venustech researcher
* Eeye researcher
* Microsoft researcher
* Vulnhunt CEO



CONTENT

- Vulnerability and APT
- APT attack analysis
- APT attack detection

Vulnerability、EXP、Shellcode、Trojan



Vulnerability and attack/defense

* Attacker
  * discover vulnerability
  * Vulnerability exploitation
  * Trojan Bypass Protection(use defense flaw)
  * Ascendant: Remote(low cost, difficult detecting, difficult forensics, difficult Law enforcement)

Defender

* Reduce vulnerability
* Detect Exp and Shellcode
* Detect the behavior of Exp and Shellcode
* Detect Trojan horse
* Detect the behavior of Trojan horse

Defender problems

* Reduce vulnerability
  * Security Development Process(Rely developer)
* Detect Exp and Shellcode
  * characteristic detection (based known, bypass)
* Detect the behavior of Exp and Shellcode
  * NX (confront)
* Detect Trojan horse
  * Static characteristic(based known, easily confrontation)
* Detect the behavior of Trojan horse
  * High-risk Behavior(mistake , confront)

CONTENT

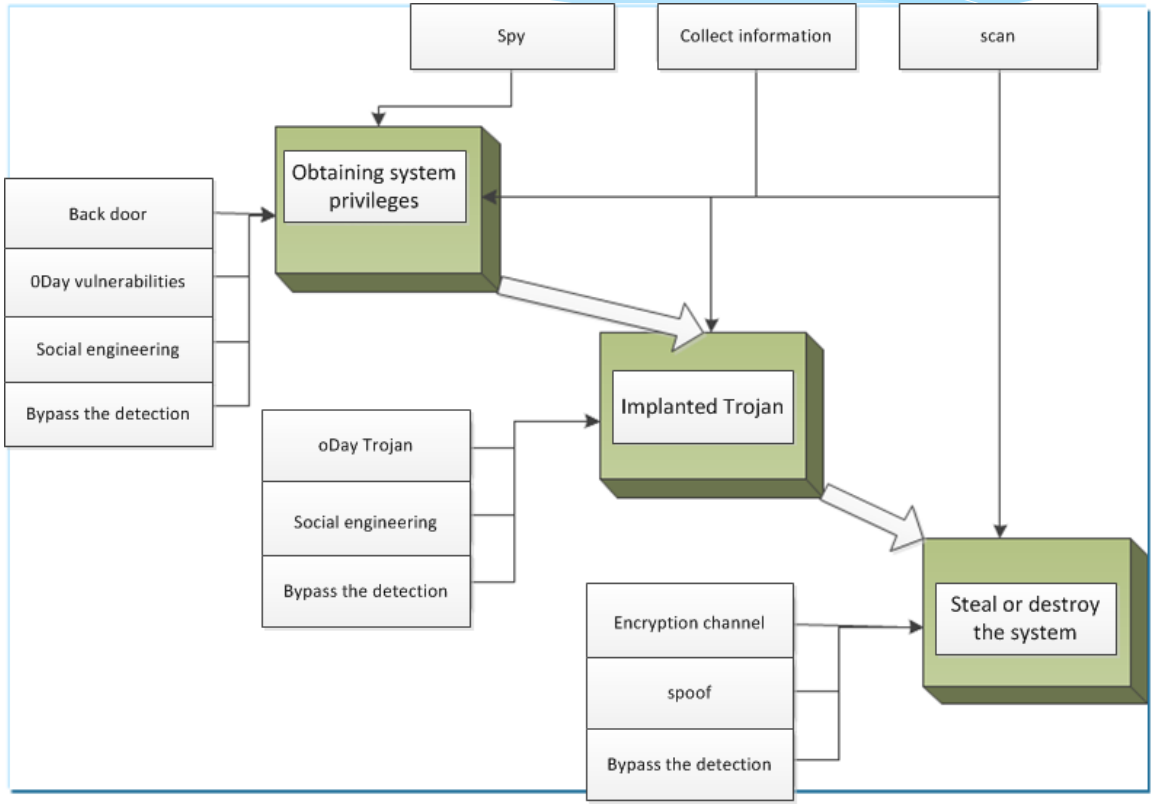
- Vulnerability and APT
- APT attack analysis
- APT attack detection

What's APT

* Advanced Persistent Threat
  * Advanced
    * Intelligence gathering and analysis
    * Social engineering
    * Professional attack techniques
  * Persistent
    * Purpose
    * Big profit
    * Organized
    * Capital adequacy

Advance Consideration

* A
  * Means
    * Spy
    * Collect information
    * Scan
    * Social engineering
    * Spoof
    * Back door
  * Techniques
    * oDAY Vulnerabilities
    * oDAY Trojan
    * Encryption channel
    * Bypass the detection



APT CASE

Google

2009：Aurora Attack

2010：Stuxnet

RSA SECURITY®

2011：Steal RSA Token

Why we can't stop them?

NASA

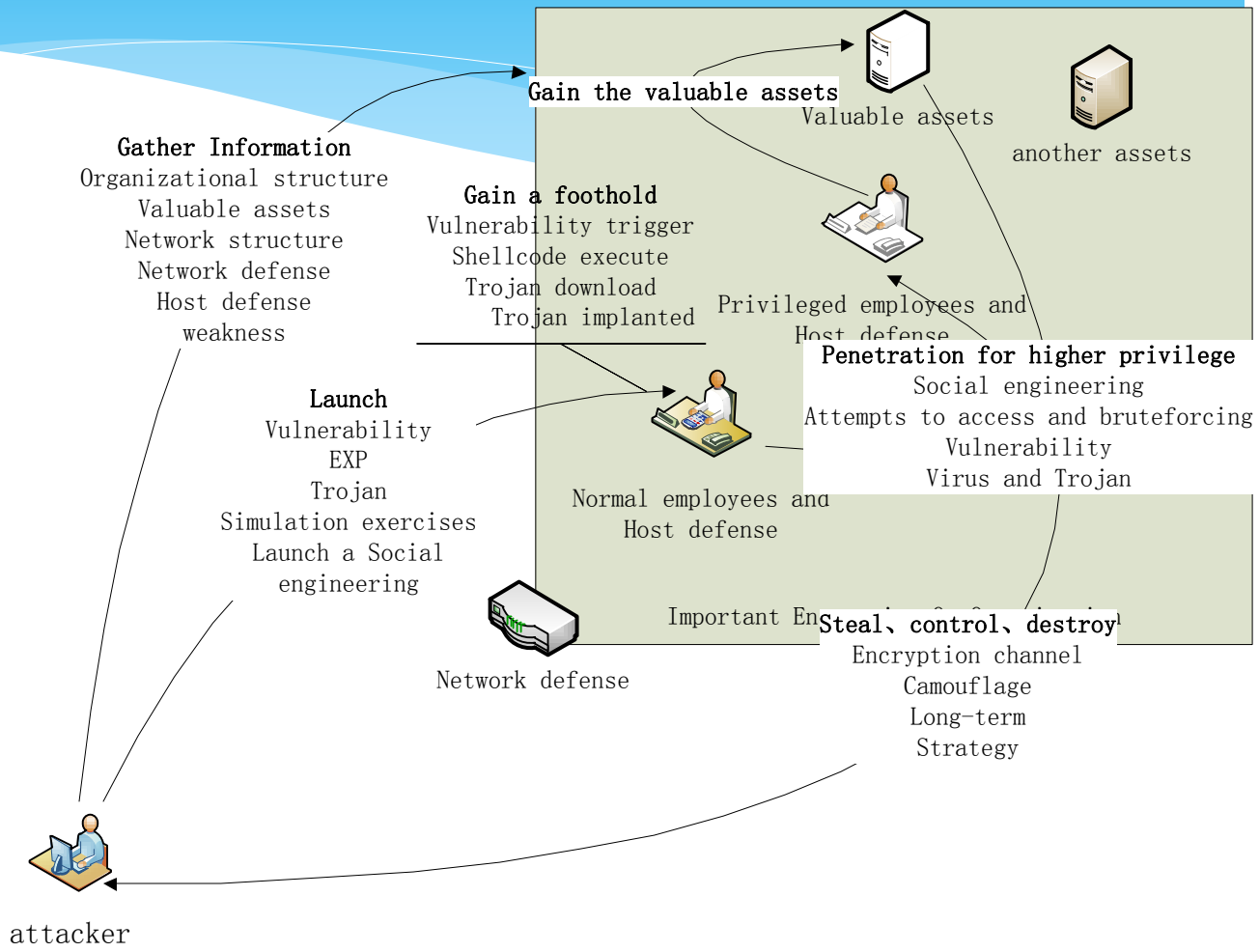
2012：Steal NASA

Flame COOKING WITH FIRE

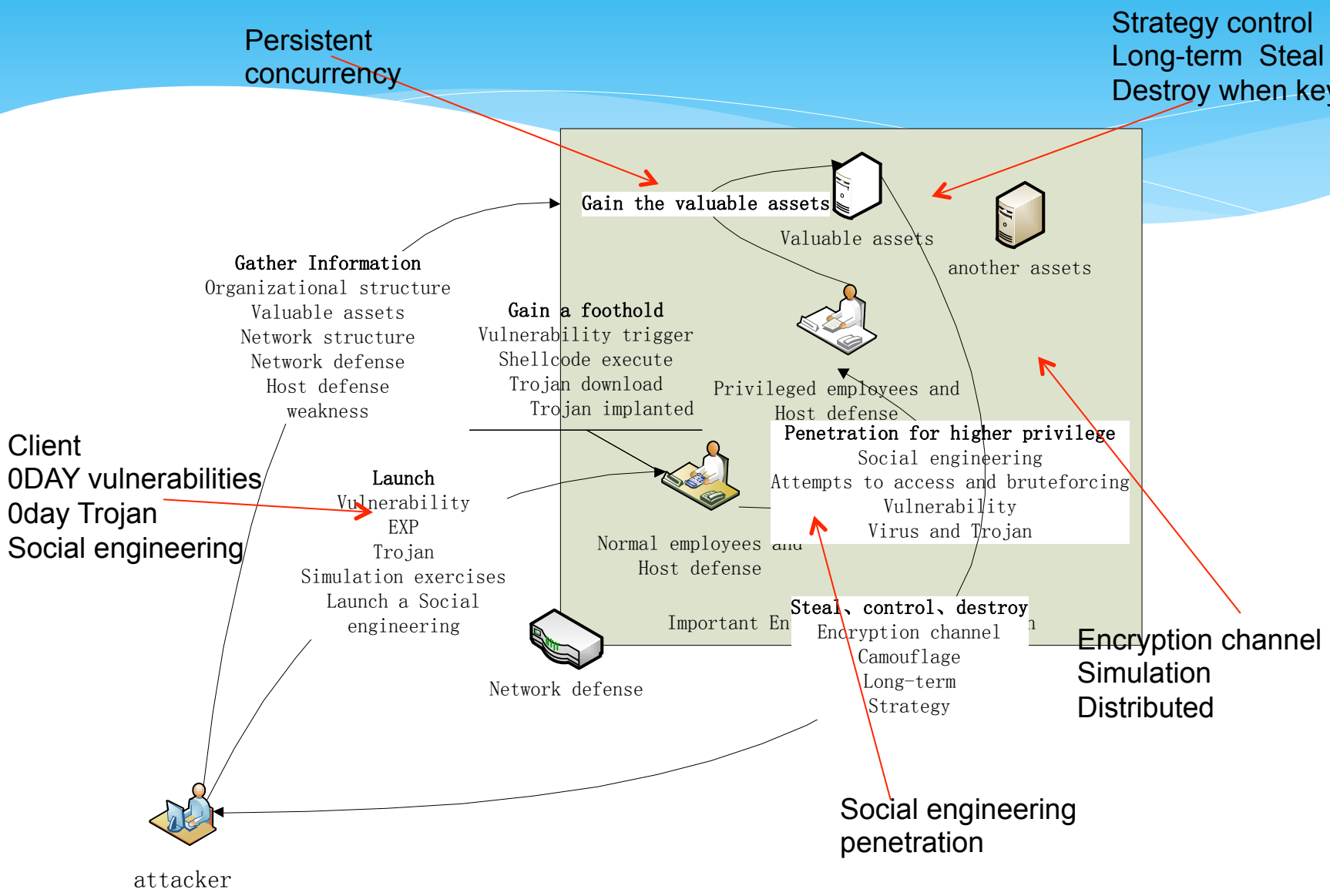
2012：Flame

APT attack process

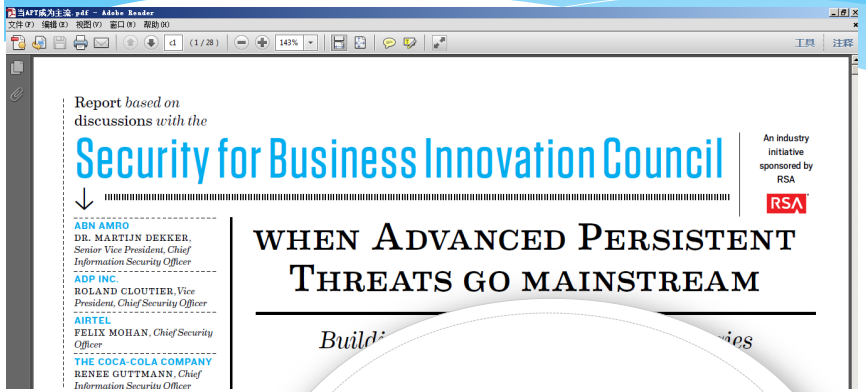
* Gather Information
* Launch
* Gain a foothold
* Penetration for higher privilege
* Gain the valuable assets
* Steal/control/destroy



APT attack feature



When APT go mainstream



Report *based on* discussions *with the*

Security for Business Innovation Council

An industry initiative sponsored by RSA

ABN AMRO
DR. MARTIJN DEKKER, *Senior Vice President, Chief Information Security Officer*

ADP INC.
ROLAND CLOUTIER, *Vice President, Chief Security Officer*

AIRTEL
FELIX MOHAN, *Chief Security Officer*

THE COCA-COLA COMPANY
RENEE GUTTMANN, *Chief Information Security Officer*

WHEN ADVANCED PERSISTENT THREATS GO MAINSTREAM

Energy
Military industry
Financial
Science research
Large manufacturing
IT
Government
Military
……

Goals:
large organizations
important information assets

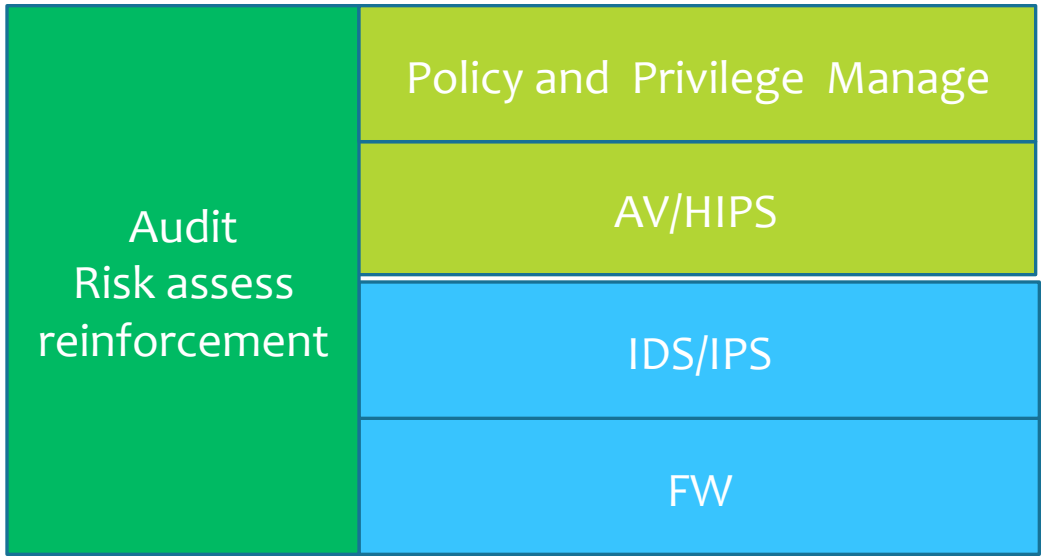
Attack path:
personal terminal
social engineering
penetration

Techniques
0day vulnerabilities
0day Trojan
encryption channel

aurora：1 0day VUL，0DAY Trojan
Stuxnet：7 0DAY VUL，0DAY Trojan
RSA：1 0DAY VUL，0DAY Trojan
flame：1 0DAY VUL，0DAY Trojan
……

Current defense system is difficult to detect and defend

The flaw of current defense system



Based known :
Known vulnerabilities
Known Trojans
Known attack behavior
Sensitive keywords

Difficult:
0day vulnerabilities
0day Trojans
Farraginous attack behavior
Encryption channel
Social engineering

Key technical point of APT Detection

Encryption channel

Unknown Trojan

Vulnerability exploitation (include oday)

Social engineering

CONTENT

- Vulnerability and APT
- APT attack analysis
- APT attack detection

APT defense technology

SDL and security testing

Vulnhunt xingyun product

	Security develop	Security testing	Security awarenes s	Security reinforc ement	FW	IPS + Vulnerability attack detection	AV + oDAY Trojan detectio n	Audit + encrypti on channel detectio n	Honeypo t + APT forensics
scan					√	√			
gather			√	√					
Social engineer ing			√						
vulnerabi lity	√	√		√		√			√
Trojan		√				√	√		√
Call back							√	√	√
destroy							√		√

Preve ntion

Detect ion

suppr ess

Respo nse

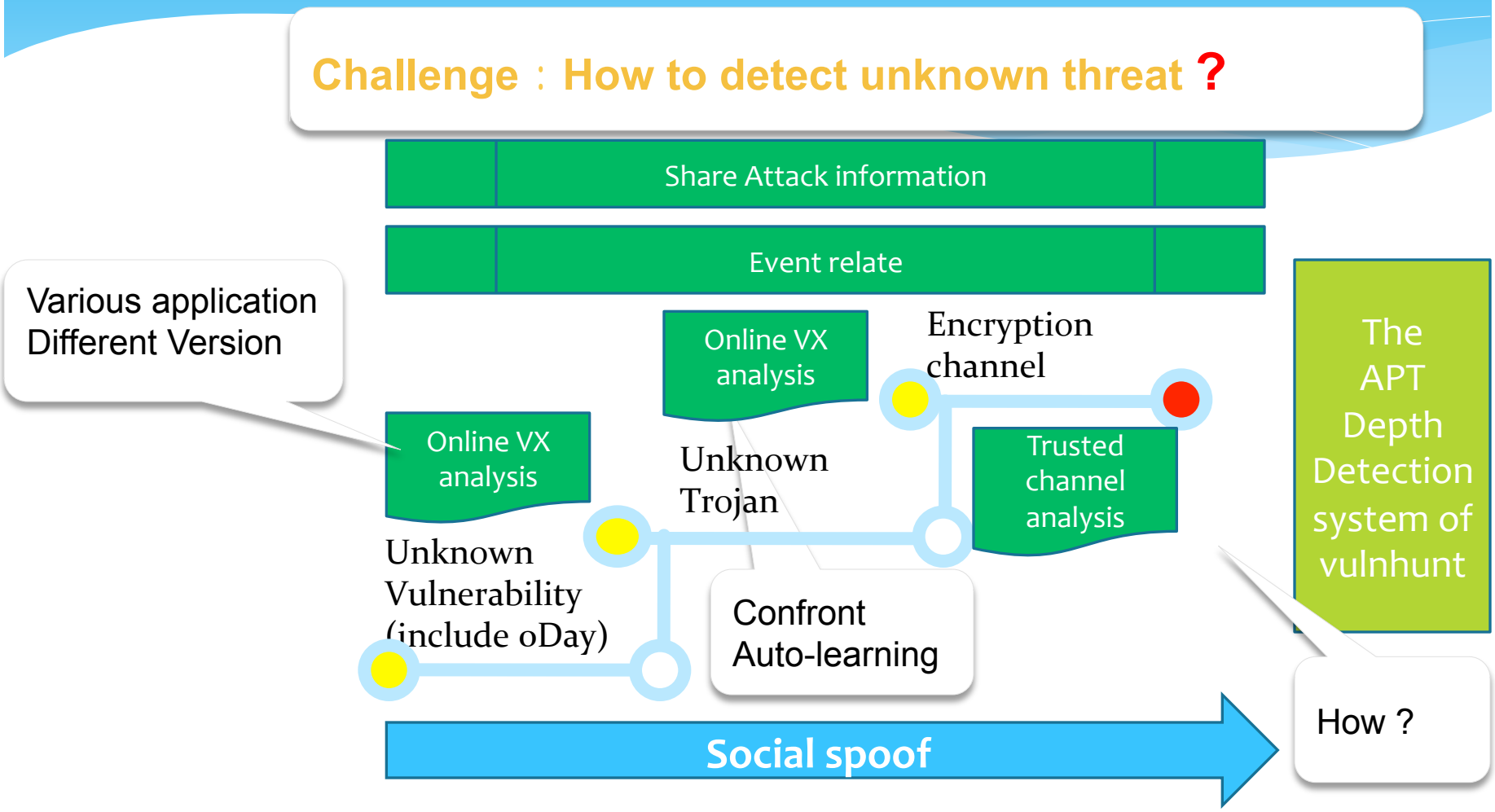
The Problem of current APT detection

* Focus point of Industry
  * oday Trojan detection
    * White list
    * Online virtual execution analysis

* Problem： hardly dominant in the confrontation
  * Detection:
    * Trojan can execute confront code
      * Example: cover up, Hijack DLL files of trusted program
    * Trojan use runtime Behavior
      * Example: Cloud push, implanted vulnerability
  * Analysis and Tracking:
    * Cloud push

The APT detection system of vulnhunt

Challenge：How to detect unknown threat ?



vulnerability attack Detection of Vulnhunt VX (include oday)

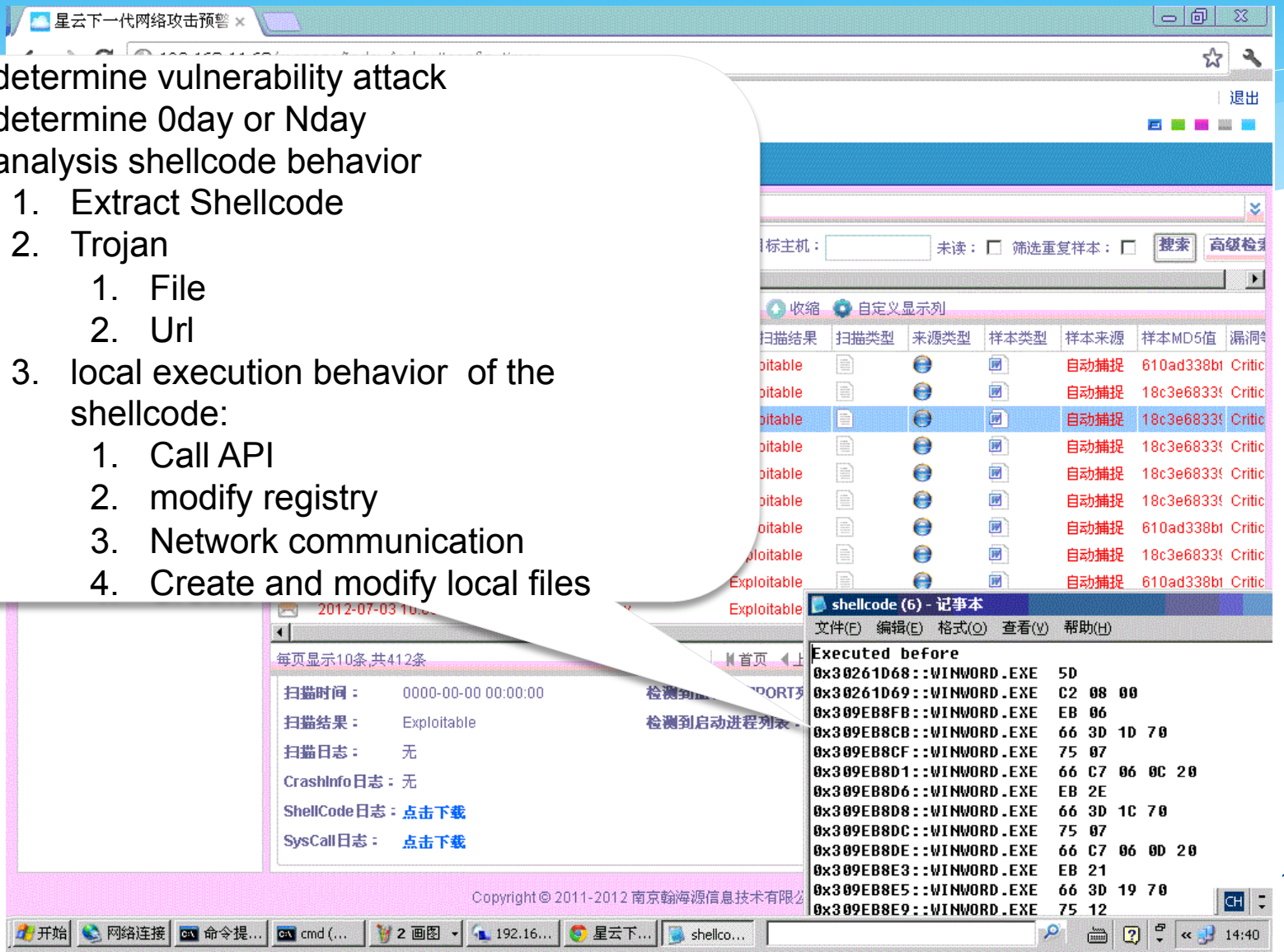
* Pre-analytical techniques of Vulnhunt
  * Embed execution code
  * Check Suspected Shellcode
    * Decode
    * Binary shellcode
      * Data seem as execution code
      * Memory Virtual Execution : independent of application
    * Script shellcode
      * Characteristic detect
      * Limited and widely known applications

vulnerability attack Detection of Vulnhunt VX (Include oday)

* VX-analysis techniques of vulnhunt
  * Determine
    * Execution Behavior : data memory execute , create process
    * Memory check : independent of version and decoding knowledge
  * Behavior recode
    * Execution recode
    * Memory Virtual Execution recode
      * binary shellcode
      * the virtual machine isn't installed this application
      * the shellcode not executed successfully

Demo of vulnhunt APT detection

1. determine vulnerability attack
2. determine 0day or Nday
3. analysis shellcode behavior
    1. Extract Shellcode
    2. Trojan
        1. File
        2. Url
    3. local execution behavior of the shellcode:
        1. Call API
        2. modify registry
        3. Network communication
        4. Create and modify local files



Trojan Detection of Vulnhunt VX (include 0day Trojan)

* Pre-analytical techniques of Vulnhunt
  * Source
    * Embed execution file
    * Execution file obtained from Email / IM /online copy/ Download
  * Known Trojan detection
    * Anti-virus
  * Self-learning detection
    * Same URL with Shellcode download
    * Same MD5 with Shellcode released

Trojan Detection of Vulnhunt VX (include 0day Trojan)

* VX-analysis techniques of vulnhunt
  * Execution behavior analysis
    * API
    * Network communication
    * Registry
    * create or modify local files
    * Resource (ex. Pipe, mutex)
  * Known Trojan Signature matched
  * Self-learning
    * Shellcode download or release files -> Trojan (white list exclude)
    * URL
    * MD5
    * Behavior recode

Encryption channel Detection of Vulnhunt (study)

* Non-encryption protocol ;encrypted data
  * Entropy analysis
* Encryption protocol ;encrypted data
  * Source exception
    * Time
    * Flow
    * Access rule
  * Destination exception
    * White list
    * Internet-aware
      * Whois analysis
      * traffic 、 link or other information

Thanks

* About Vulnhunt Inc.
  * Founded in 2010.6, flashsky & alert7
  * Business
    * Security testing service
    * SDL service
    * APT attack Detection product
    * Customers
      * HuaWei ,Tencent ,Kingsoft ,360 …..
* Thanks
* Email : xing_fang@vulnhunt.com
* Q/A