Malware Analysis

By Z-Lab team

ISWATLab

Outline

- About us
- Definitions
- Threat Intelligence
- Platforms
- Malware Analysis

About us

- Z-Lab
  - The malware lab of CSE CybSec Enterprise spa

- Core Team

Antonio Pirozzi, Director

antopirozzi@gmail.com

Luigi Martire, Malware Analyst

luigimartire94@gmail.com

Antonio Farina, Malware Analyst

antoniofarina1702@gmail.com

About us

- What we do

CSE Malware ZLab – Preliminary analysis of Bad Rabbit attack

October 25, 2017 By Pierluigi Paganini

My Page

We at the CSE Cybsec ZLab have conducted a preliminary analysis of the Bad Rabbit ransomware discovering interesting aspects of the attack.

Exclusive – CSE ZLab experts spotted a new Wonder botnet in the wild

October 23, 2017 By Pierluigi Paganini

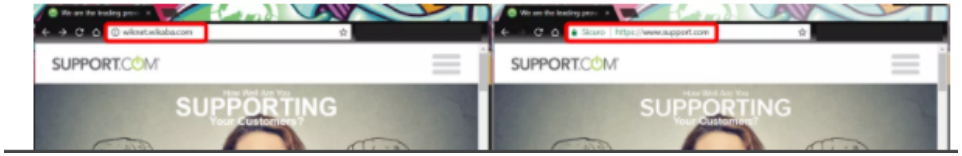
My Page

The CSE CybSec Z-Lab Malware Lab spotted a new botnet, dubbed Wonder botnet, while it was investigating malicious code in the dark web.

While investigating the malicious code in the dark web, ZLab experts discovered a "NetflixAccountGenerator.exe" that promises to generate a premium account for Netflix services for free. Unfortunately, the software downloaded does not work as expected because it installs a BOT rather than create a desiderated account!

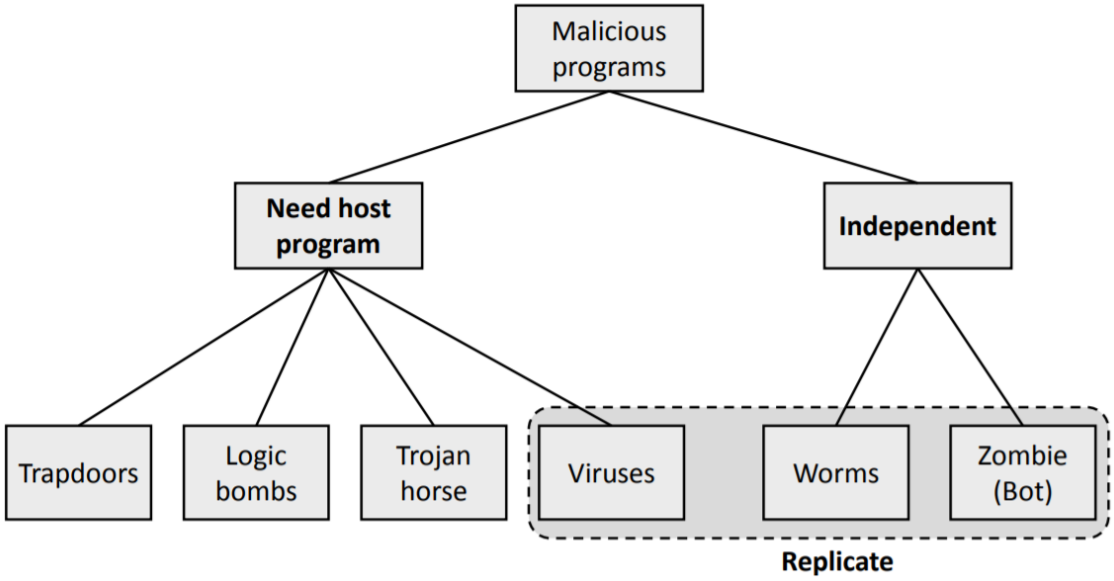
The malware researchers analyzed this "exe" file and discovered that the malware is not indexed yet: only one site on the Clearnet identified it as a threat after it was uploaded for the first time around September 20th, probably by the author in order to test its ability to remain stealth.

The analysis of the malware revealed it is a bot that belongs to an alive botnet dubbed by the experts Wonder botnet. The Command and Control is hidden behind a site that is the mirror of another one:



Malware

- Malware is
  - a set of instructions that run on your computer and make your system do something that someone wants it to do.



Malware (2)

- Malwares hit every system

the paranoids survive»

Andrew Grove

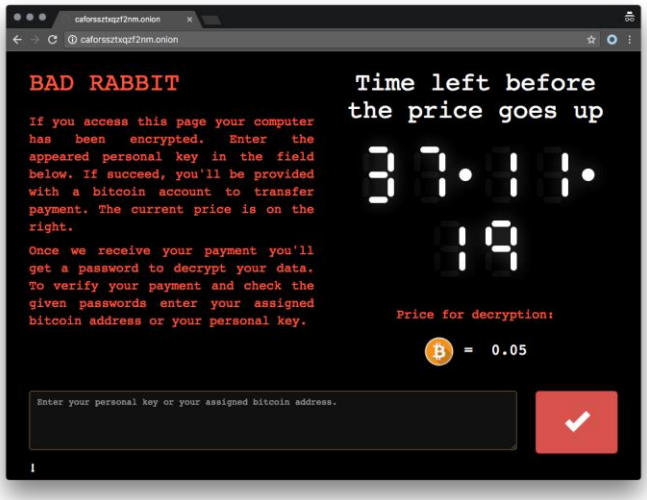
Palo Alto Networks Blog

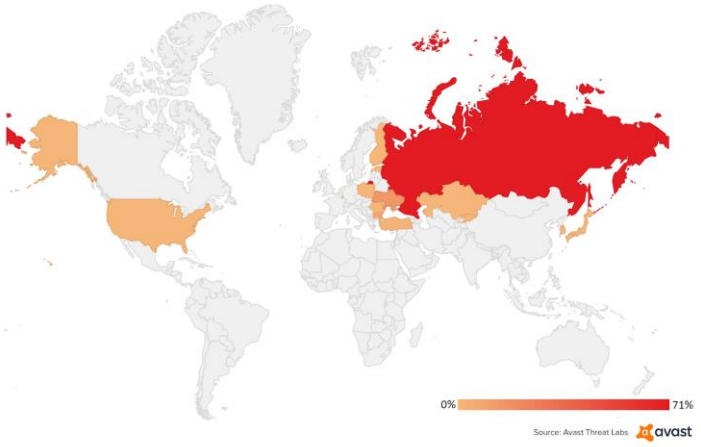
AceDeceiver: First iOS Trojan Exploiting Apple DRM Design Flaws to Infect Any iOS Device - Palo Alto

https://objective-see.com/malware.html

Malware (3)

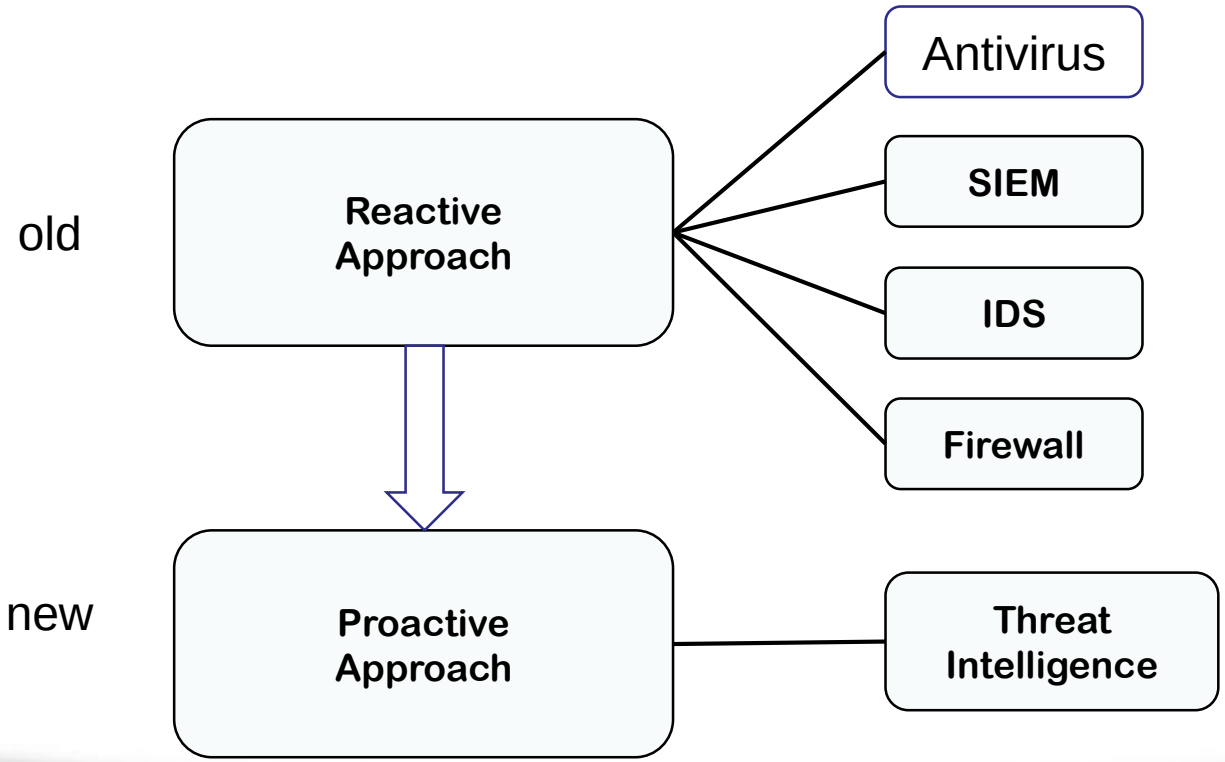
- Motivations
  - Money
    - Ransom payment
    - Third part requests
    - Cyber espionage
  - Power
    - Cyberwarfare
    - State sponsored
    - Personal pleasure





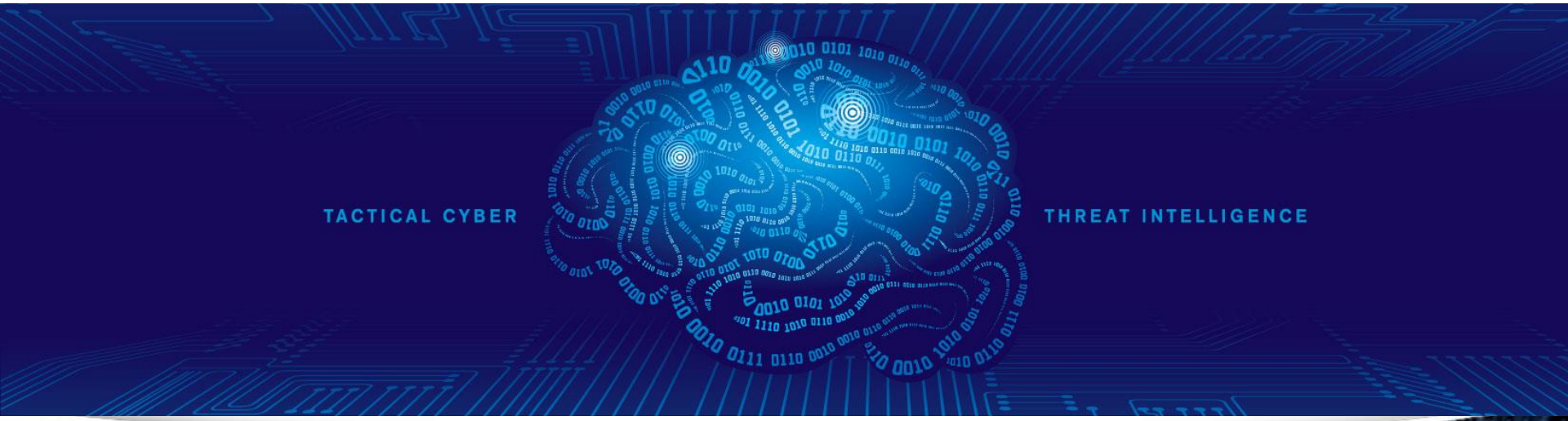
Threat Intelligence

- The question is not if but when!
  - New approach to opposite malware attacks

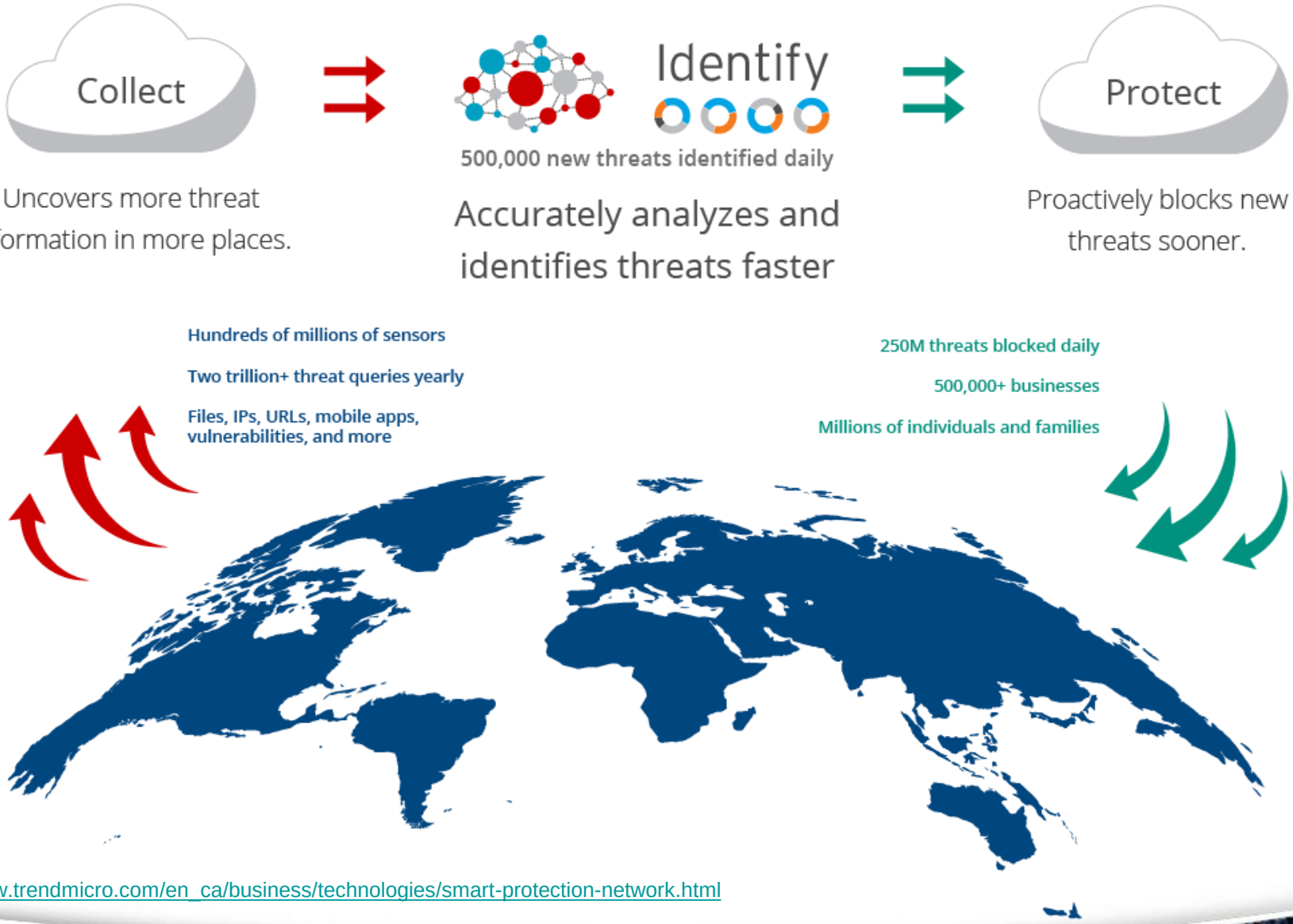


Threat Intelligence

- We must face off new threats collaborating with other many entities.
- It is necessary a continous and timely sharing of knowledge



Threat Intelligence



Source:
https://www.trendmicro.com/en_ca/business/technologies/smart-protection-network.html

Threat Intelligence

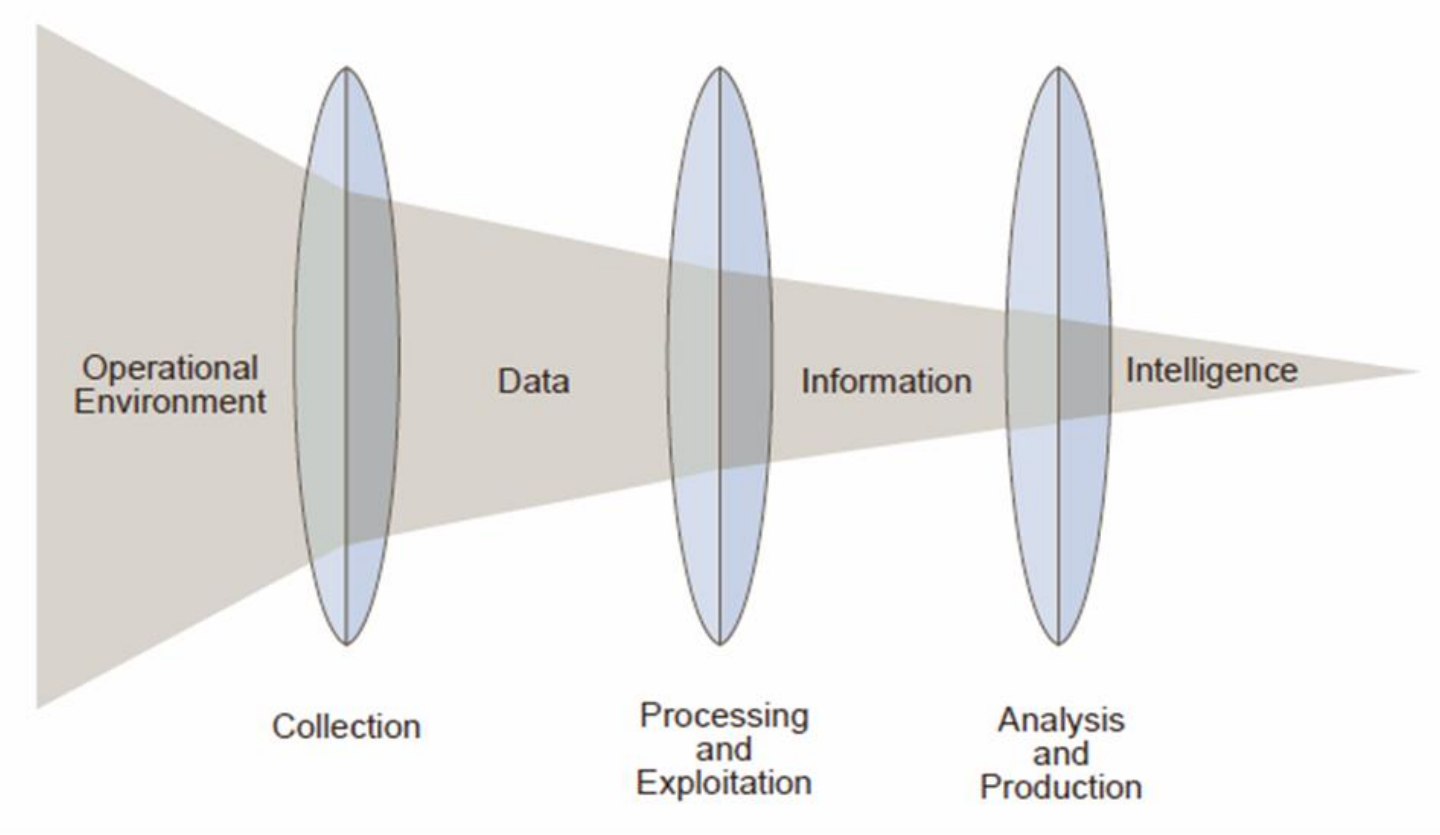
- Threat intelligence is created by a process which takes raw data and information from a variety of sources and turns it in to strategically, tactically or operationally valuable information.
- The typical sources of this raw data and information often include:
  - Human-supplied: human intelligence (HUMINT).
  - Internet-published: open-source intelligence (OSINT)
  - Network-traffic-derived: signals intelligence (SIGINT).
  - Technical artefacts: cyber-intelligence (CYBINT) or cyber-specific technical intelligence (TECHINT).

OSINT

- Open Source INTelligence (OSINT)
  - collection of information and sources that are generally available, including information obtained from the media (newspapers, radio, television, etc.), professional and academic records papers, conferences, professional associations, etc.), and public data (government reports, demographics, hearings, speeches, etc.). Cit. FBI

OSINT

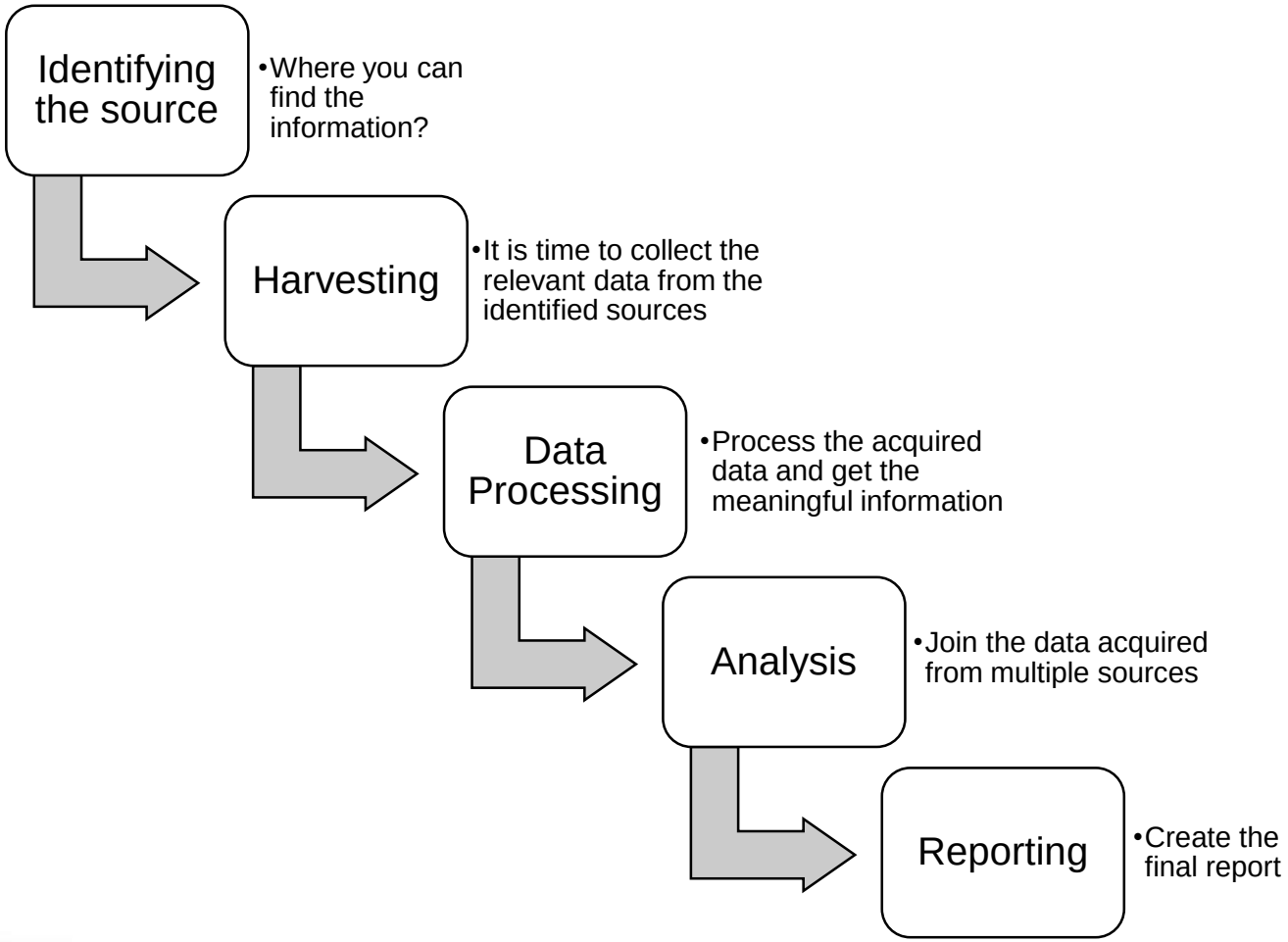
- Process of structuration of an information



Source: Joint Intelligence / Joint Publication 2-0 (Joint Chiefs of Staff)

OSINT

- The OSINT Process



- Hostnames
- Services
- Networks
- SW/HW versions and OS information
- GEO-Location
- Network Diagram
- Database
- Documents, papers, presentations, and configuration files
- Metadata
- Email and employee search (name and other personal information)
- Technology infrastructure
- IP

Threat Intelligence

- “Threat intelligence is the output of analysis based on identification, collection, and enrichment of relevant data and information regarding cyber attacks.”
- Threat intelligence falls into two categories.
  - Operational intelligence is produced by computers
  - Strategic intelligence is produced by human analysts.

- The two types of threat intelligence are heavily interdependent

Threat Intelligence

- Operational Intelligence:
  - A common example of operational threat intelligence is the automatic detection of distributed denial of service (DDoS) attacks, whereby a comparison between indicators of compromise (IOCs) and network telemetry is used to identify attacks much more quickly than a human analyst could.
- Strategic Intelligence:
  - focuses on the much more difficult and cumbersome process of identifying and analyzing threats to an organization's core assets, including employees, customers, infrastructure, applications, and vendors.

Threat Intelligence

- What share?
  - Indicators of Compromise – IoC
    - «is an artifact observed in a system or on a network that with high confidence indicates a compromission»
    - IP, URLs, Virus signatures, Hashes, Malware files
  - Tactics, Techniques and Procedures – TTP
    - «Are representations of the behavior or modus operandi of cyber adversaries»
  - Report
  - IDPS rules

Threat Intelligence

- How share?
  - OpenIoc
  - Yara
  - TAXII
  - Stix
  - Cybox

Source:
https://threatpost.com/misunderstanding-indicators-of-compromise/117560/

Threat Intelligence

- Yara rules example

```
import "pe"

rule BadRabbit_dropper {

    meta:
        description = "Yara Rule for Bad Rabbit dropper identification"
        author = "CSE CybSec Enterprise - Z-Lab"
        last_updated = "2017-10-31"
        tlp = "white"
        category = "informational"

    strings:
        // Flash string
        $flash = "Flash" wide

        // File infpub extracted
        $a = "C:\\Windows\\infpub.dat" wide
        $b = "infpub.dat" wide

        // Execution of infpub.dat
        $c = "%ws C:\\Windows\\%ws,#1 %ws" wide

    condition:
        all of them and
        pe.version_info["ProductName"] contains "Installer/Uninstaller"

}
```

Threat Intelligence Platforms

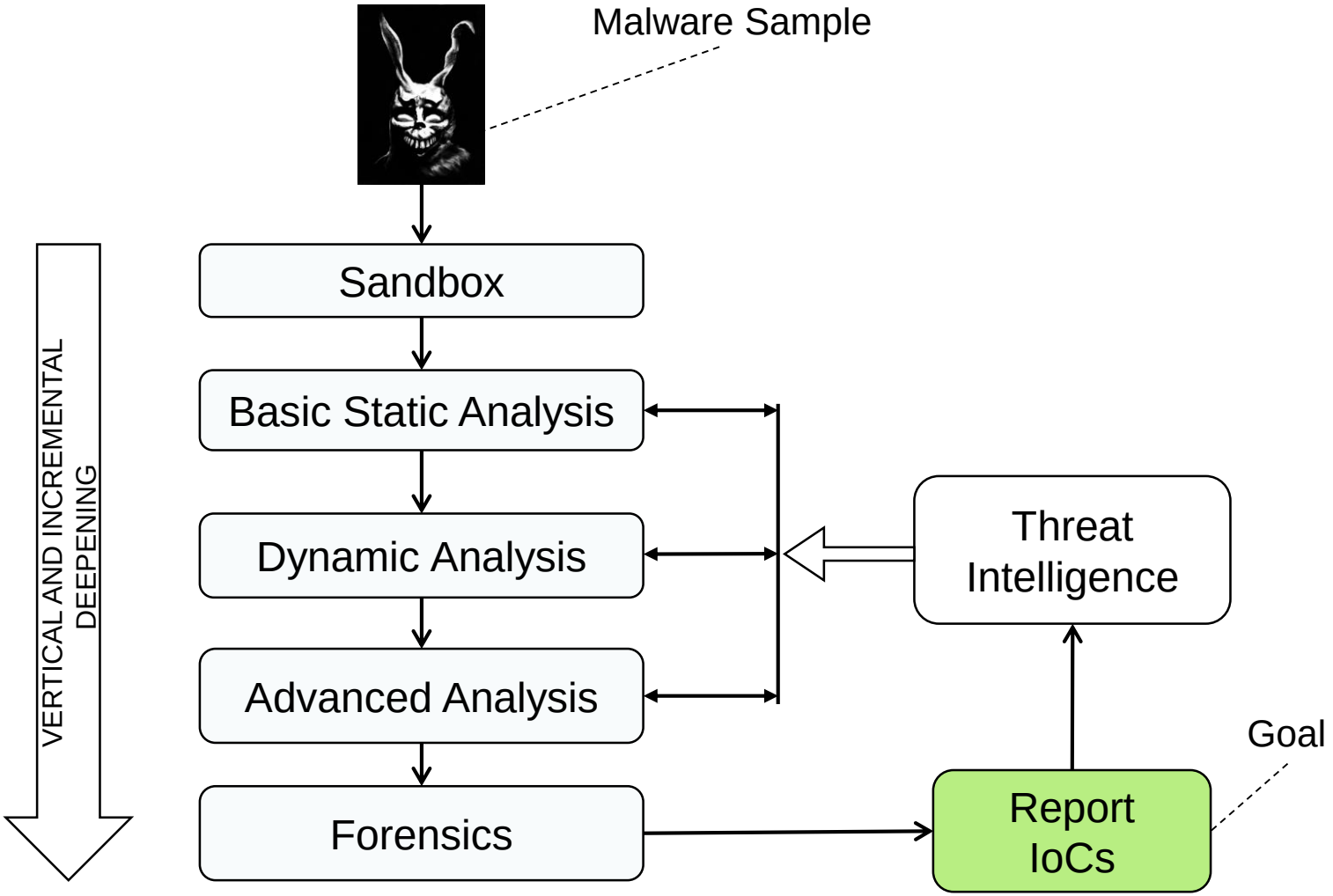
- Where share?
  - OTX by Alienvault
  - XForce by IBM
  - MISP
  - Anomali
  - Threatcrowd
  - Threatconnect
  - Blueliv

Blueliv.

Threat Intelligence & IoC

- How extract malwares' IoCs and other characteristics to share?

The Malware Analysis Process



Malware Sample

Retrieve malware from:

- Infected machines
- Disk images
- Network traffic
- Suspicious files
- Public sources
- Deep web
- HoneyNet

Sandbox

- Submit the sample into Cuckoo Sandbox private instance or Payload Security
- Malware’s first impressions and initial triaging

Basic Static Analysis

- Retrieve the first info's about the characteristics of the malicious file:
  - FileType
  - Hashes
  - Strings
  - Sections
  - Imports
  - Packers

Dynamic Analysis

- Observe the malware in action:
  - Runtime API calls
  - Network Traffic
  - Files' accesses
  - Registry Keys' accesses
  - System settings alteration
  - Disk Modification
  - Lateral movements
  - Privilege Escalation

Advanced Analysis

- Advanced Static&Behavioural Analysis
  - Refine the characteristics of the malware through the correspondence of the malware execution in a debugger with its disassembled code
  - Find particular structures and IoC in the malware's code

Forensics

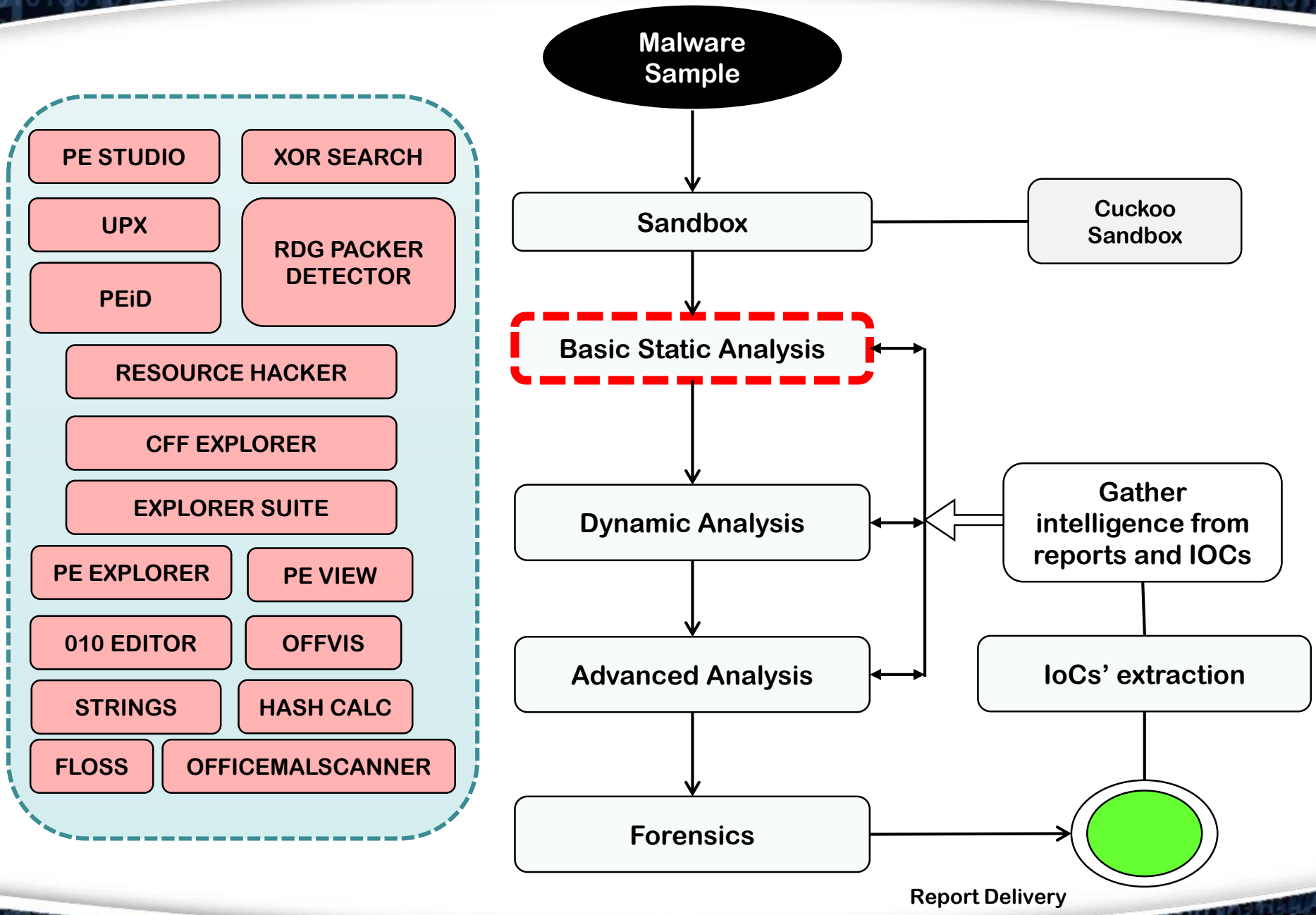
- Extract evidences and digital artifacts from various supports
  - Disk
  - Memory
  - Volatility Framework

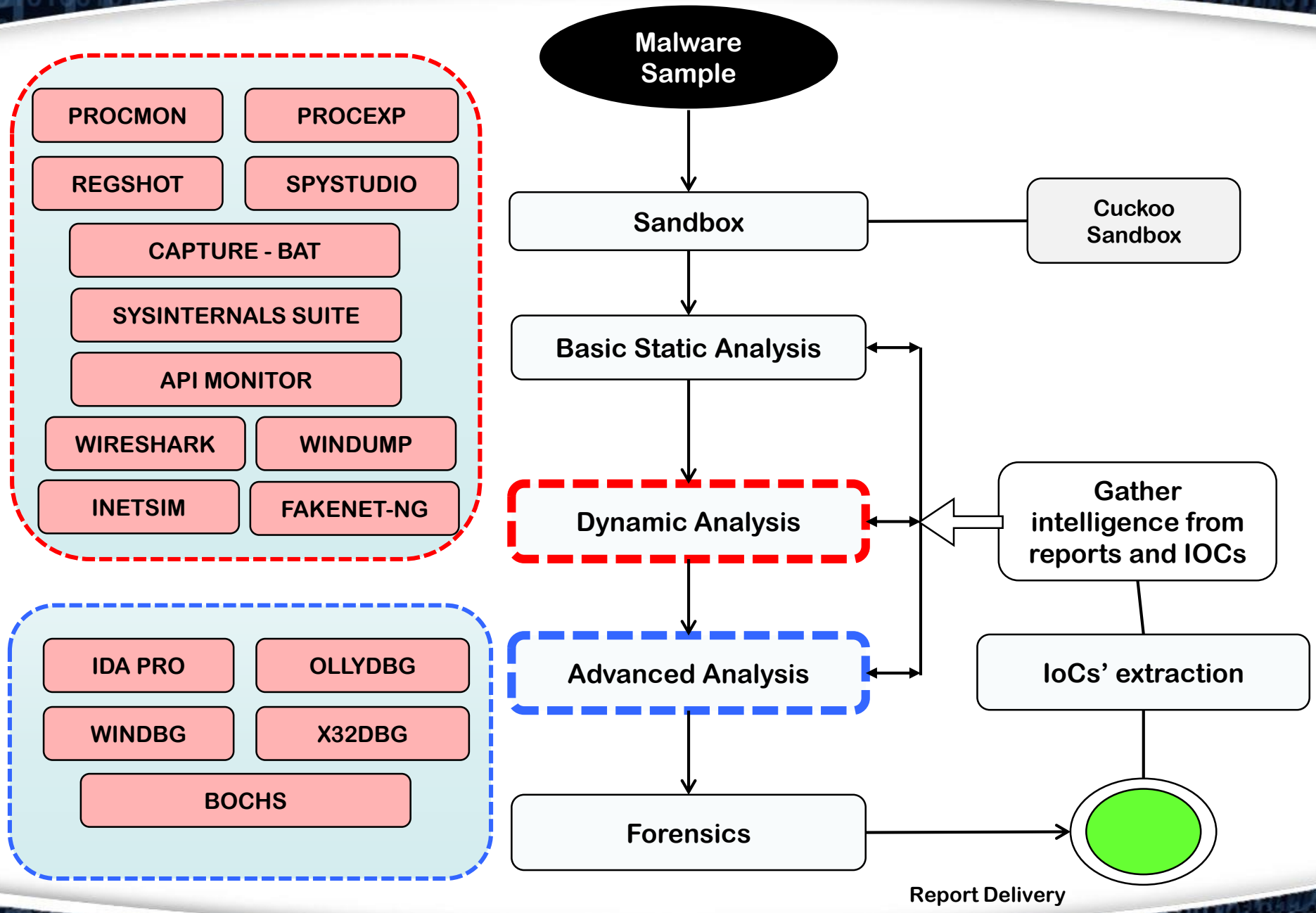
IoC extraction

- Synthetize the info about malwares to recognize them in rules that allow their detection
  - Yara
  - OpenIoC

Gather intelligence from reports and IoCs

- Take comparison in all previous steps between the info gathered in various Threat Intelligence Platforms and those extracted during the analysis
  - Compare hashes
  - Compare behaviour
  - Compare IoCs


Malware Sample
Sandbox
Cuckoo Sandbox
Basic Static Analysis
Dynamic Analysis
Gather intelligence from reports and IOCs
Advanced Analysis
IoCs' extraction
Forensics
Report Delivery
PE STUDIO
XOR SEARCH
UPX
RDG PACKER DETECTOR
PEiD
RESOURCE HACKER
CFF EXPLORER
EXPLORER SUITE
PE EXPLORER
PE VIEW
010 EDITOR
OFFVIS
STRINGS
HASH CALC
FLOSS
OFFICEMALSCANNER


Malware Sample
Sandbox
Cuckoo Sandbox
Basic Static Analysis
Dynamic Analysis
Advanced Analysis
Forensics
Gather intelligence from reports and IOCs
IoCs' extraction
Report Delivery
PROCMON
PROCEXP
REGSHOT
SPYSTUDIO
CAPTURE - BAT
SYSINTERNALS SUITE
API MONITOR
WIRESHARK
WINDUMP
INETSIM
FAKENET-NG
IDA PRO
OLLYDBG
WINDBG
X32DBG
BOCHS