Network Security
(6CCS3NSE - 7CCSMNSE)

Diego Sempreboni
Department of Informatics
King's College London, UK

Second term 2019/20
Lecture 6

Objectives and learning outcomes

- Understand the difference between firewalls and IDPSs
- Be able to classify the different types of IDPSs
- Understand the importance of OSINT
- Know basic evasion techniques
- Distinguish between the different type of Honeypots

Intrusion: definitions

- **Intrusion:** unwanted and unauthorised **intentional** access of computerised network resources

- **Intrusion detection:** detecting unauthorised use of a system or network, detecting attacks upon a system or network

- **Intrusion detection system (IDS):** does for network what AVs do with incoming files
  - Components: sensors, alerts

Intrusion: definitions

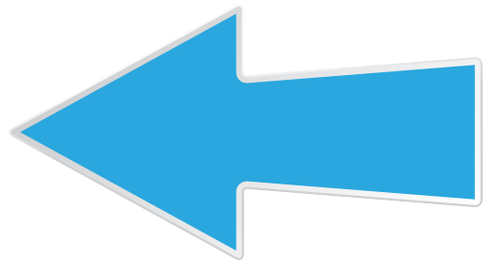
- **Intrusion Prevention System (IPS):** an IDS with an automated response
  - Shut down attacker connections
  - Try to back-trace attacker
  - Counter-attack

- **Intrusion Detection and Prevention System (IDPS):**

IDPS classification

- Timeliness:
  - Real-time (on-line, continuously, running)
  - Non real-time (off-line, periodic)

- Response type:
  - Passive (generates alerts)
  - Active (blocks malicious traffic)



- State-dependency:
  - Stateful analysis
  - Stateless analysis

IDPS classification

- System type:
  - Software
  - Hardware

- Detection type:
  - Reputation detection
  - Misuse detection
  - Anomaly detection

- Topology
  - Network IDS (NIDS)
  - Host IDS (HIDS)
    - Distributed IDS (DIDS) :Monitors the whole network with multiple probes (network-and/or host-based)

Reputation-based detection

- Idea: detect host communicating with a someone with bad reputation.

- Based on (public or private) blacklists:
  - Malware Domain List (MDL):
    - Google Safe Browsing or VirusTotal
  - Spamhaus Block Lists
    - http://www.spamhaus.org/drop/
  - PhishTank
    - http://www.phishtank.com/
  - Botnet trackers: abuse.ch ZeuS and SpyEye
    - https://zeustracker.abuse.ch/
    - https://spyeyetracker.abuse.ch/
  - Tor Exit Node List
    - http://torstatus.blutmagie.de/
  - ... and many more

Open Source Intelligence (OSINT)

- Data collected from publicly available sources that is used in an intelligence context

MALWARE DOMAIN LIST

Homepage | Forums | Recent Updates | RSS update feed | Contact us

WARNING: All domains on this website should be considered dangerous. If you do not know what you are doing here, it is recommended you leave right away. This website is a resource for security professionals and enthusiasts.

Search: All Results to return: 50 Include inactive sites

Search

Page 0 1 ... 22

Date (UTC)	Domain	IP	Reverse Lookup	Description	ASN	
2017/12/04_18:50	textspeier.de	104.27.163.228	-	phishing/fraud	13335	
2017/10/26_13:48	photoscape.ch/Setup.exe	31.148.219.11	knigazdorovya.com.	trojan	14576	
2017/06/02_08:38	sarahdaniella.com/swift/SWIFT%20$.pdf.ace	63.247.140.224	coriandertest.hmdnsgroup.com.	trojan	19271	
2017/05/01_16:22	amazon-sicherheit.kunden-ueberpruefung.xyz	185.61.138.74	hosted-by.blazingfast.io.	phishing	49349	
2017/03/20_10:13	alegroup.info/ntnrrhst	194.87.217.87	mccfortwayne.org.	Ransom, Fake.PCN, Ma lspam	197695	
2017/03/20_10:13	fourthgate.org/Yryzvt	104.200.67.194	-	Ransom, Fake.PCN, Ma lspam	8100	
2017/03/20_10:13	dieutribenhkhop.com/parking/	84.200.4.125	125.0-255.4.200.84.in-addr.arpa.	Ransom, Fake.PCN, Ma lspam	31400	
2017/03/20_10:13	dieutribenhkhop.com/parking/pay/rd.php?id=10	84.200.4.125	125.0-255.4.200.84.in-addr.arpa.	Ransom, Fake.PCN, Ma lspam	31400	
2017/03/14_23:02	ssl-6582datamanager.de/	54.72.9.51	ec2-54-72-9-51.eu-west-1.compute.amazonaws.com.	redirects to Paypal phishing	16509	
2017/03/14_23:02	privatkunden.datapipe9271.com/	104.31.75.147	-	Paypal phishing	13335	
2017/03/06_21:09	www.hjaoopoa.top/admin.php?f=1.gif	52.207.234.89	ec2-52-207-234-89.compute-1.amazonaws.com.	Cerber ransomware	14618	
2017/03/06_21:09	up.mykings.pw:8888/update.txt	60.250.76.52	60-250-76-52.HINET-IP.hinet.net.	related to a Mirai windows spreader trojan	3462	

Virus total

- https://www.virustotal.com/#/ip-address/71.78.24.146
- API

71.78.24.146 IP address information

Country	US
Autonomous system	11427 (Charter Communications Inc)

Passive DNS Replication

Date resolved	Domain
2019-02-06	rrcs-71-78-24-146.sw.biz.rr.com

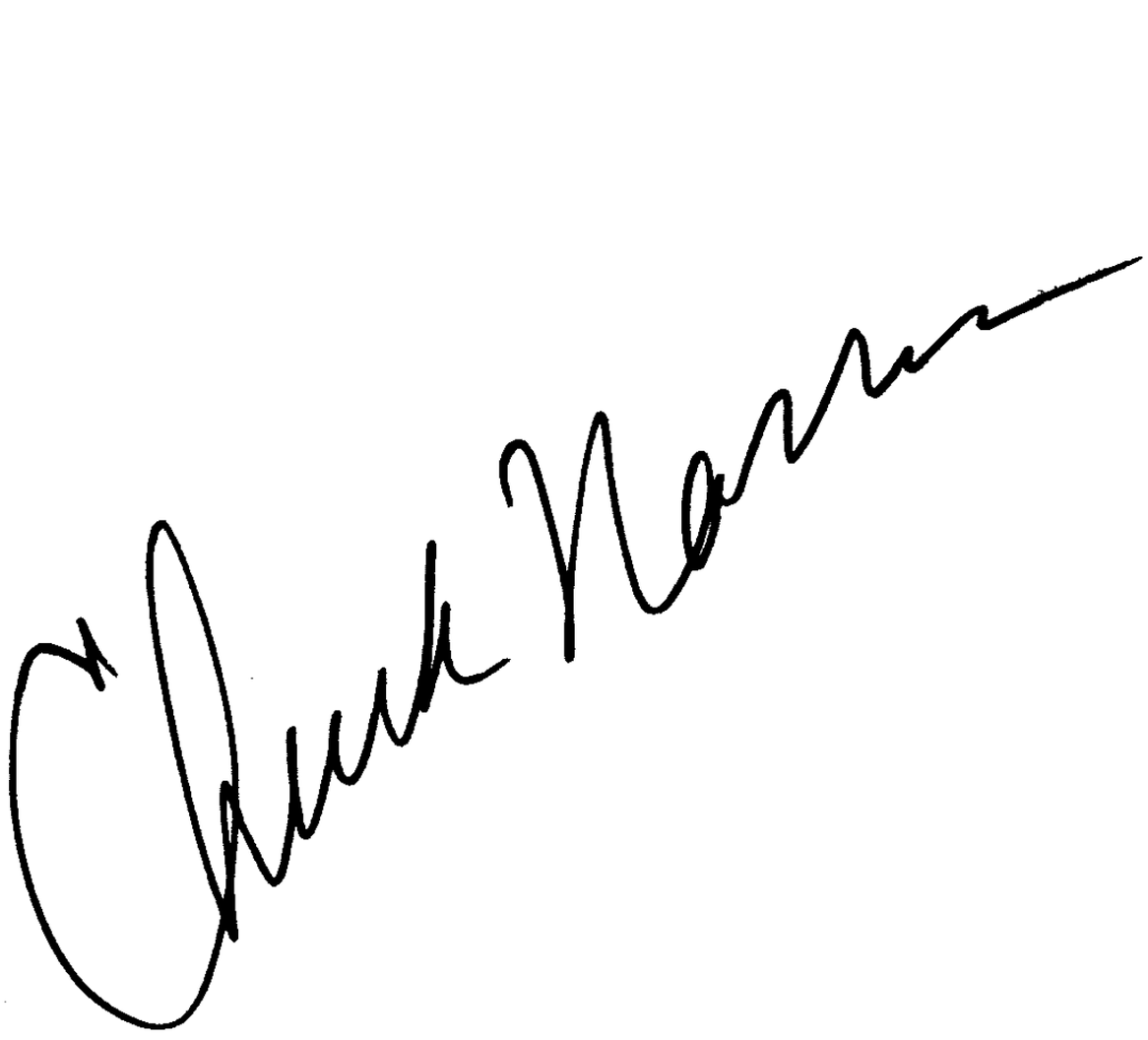
URLs

Date scanned	Detections	URL
2019-02-14	7/67	http://71.78.24.146/administration/crime_records/pages/applicantfingerprintservices.htm
2019-02-14	7/67	http://71.78.24.146/internetforms/Forms/CR-63.pdf
2019-02-18	10/69	http://71.78.24.146/
2019-02-06	6/67	http://71.78.24.146/&d=DwMFAg&c=HLbbteRuw0pQ/12aHbLLLIQMJSgQcVNjSOe1%z8k6
2019-02-05	4/69	http://71.78.24.146/http:/organikatzir.enterhello.com/2BSOzk3y02N7_no/

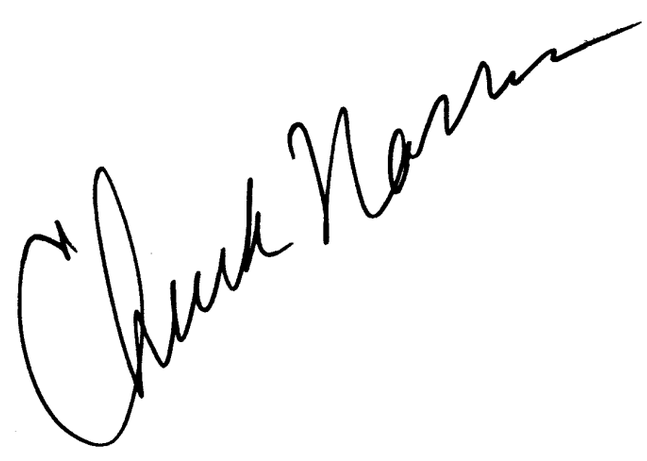
Communicating Files

Date scanned	Detections	File type	Name
2019-02-18	47/71	Win32 EXE	extractr.exe

Misuse based vs anomaly detection



A classification of Intrusion Detection Systems (IDS)



- Misuse-based
  - Rely on models of malicious behaviour (traditionally **signatures**)
  - Identify **matching entries** in the event stream
  - OSINT: Indicators of Compromise (IoC)
- Anomaly-based
  - Rely on models of normal behaviour
  - Identify **anomalous entries** in the event stream

Indicators of Compromise (IOCs)

Host-based

- Registry key
- Process name
- User account
- Directory path
- File name
- File hash
- Text string in file

Network-based

- IP address
- Port
- Protocol
- Domain name
- URL
- Downloaded file name or hash
- Text string in payload

The good and the bad

- **Misure-based detection:**
  - Generates few false alarms 
  - Provides an explanation for alerts 
  - It is fast 
  - It is (more) resilient to evasion 

  - It detects only known attacks 
  - It needs continuous updating 
  - It is vulnerable to over-stimulation attacks 

The good and the bad

- **Anomaly-based detection**
  - Detects previously-unknown attacks ☺
  - Does not need updating ☺
  - It is difficult to configure (train) ☹
  - Assumes that anomalous means malicious ☹
  - Generates many false alarms ☹
  - Does not provide identification ☹
  - Resource-intensive ☹

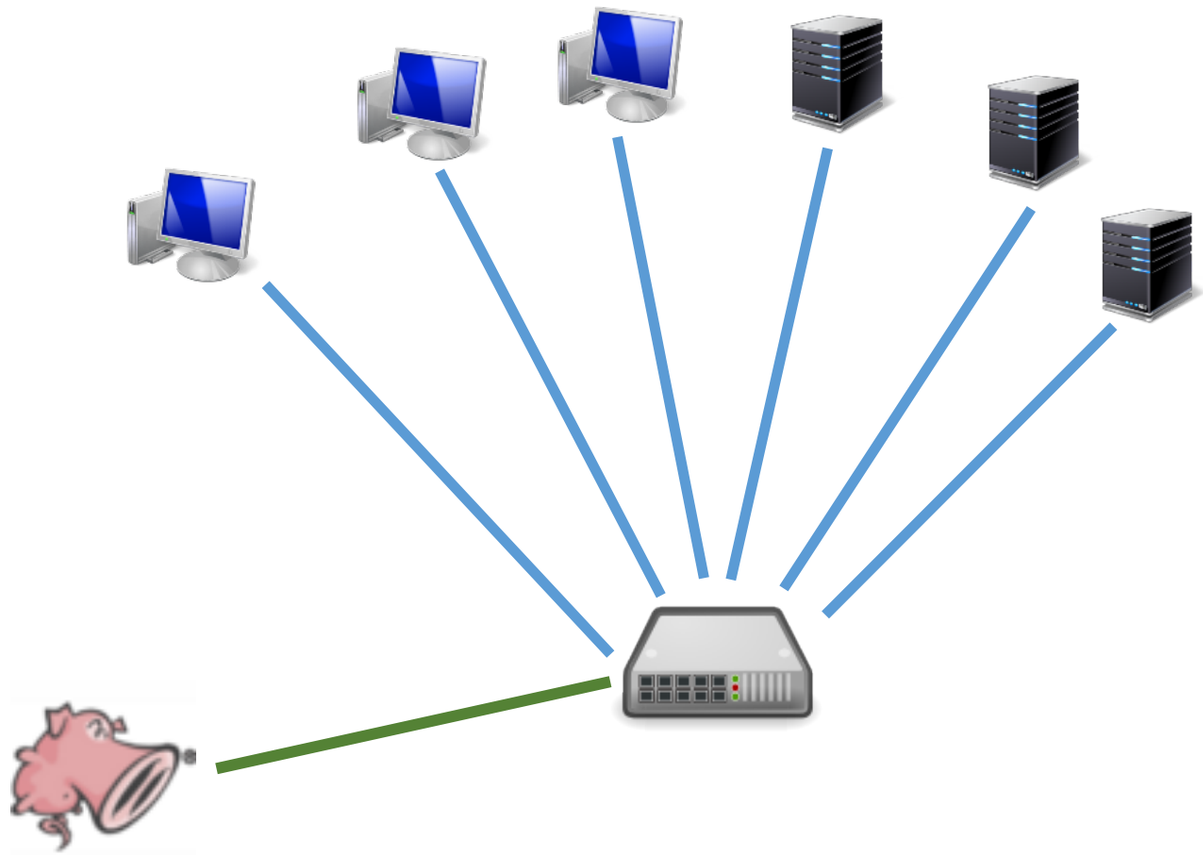
Network IDS (NIDS)

- Eavesdrop all in a network segment:
  - NIC (Network Interface Controller) in promiscuous mode
    - Not only from my NIC

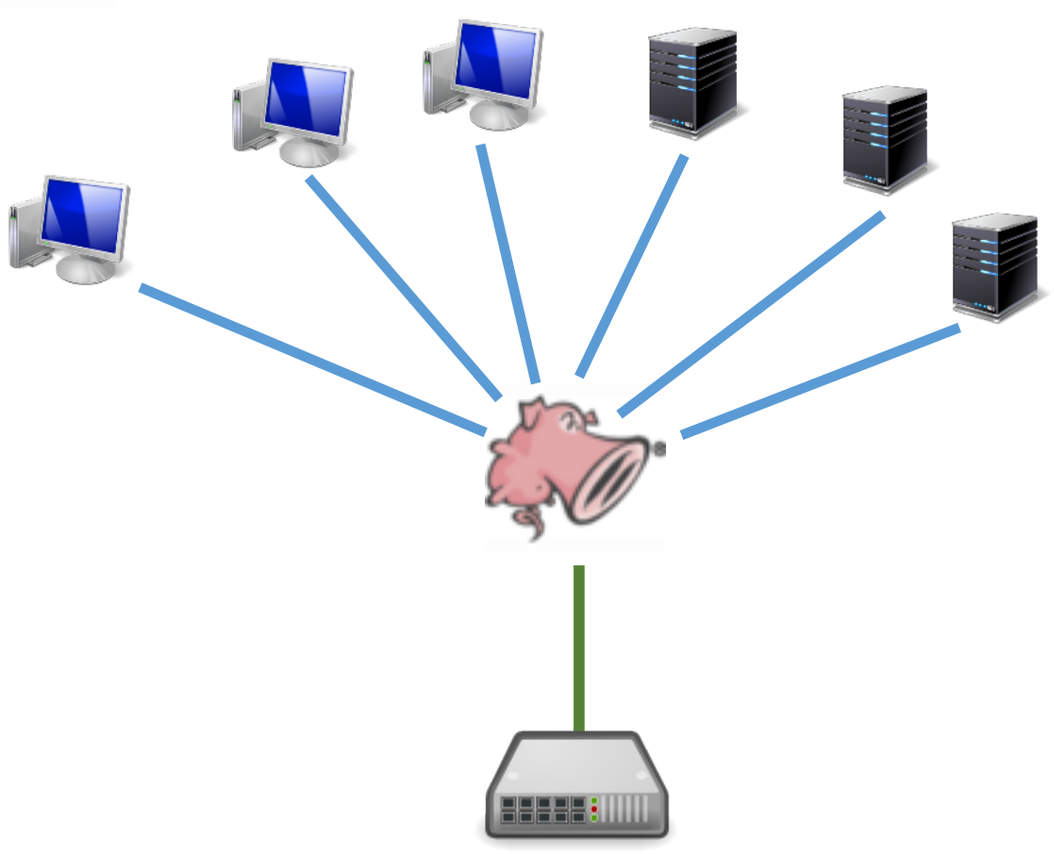
- Placed at strategic locations:
  - Choke points (like Firewalls)
  - DMZ
  - Internal networks (unlike Firewalls)

Deployment

- Traditional deployment: the IDS is connected to a trunk port and can see all the network traffic
  Can detect attacks, no countermeasures



- Inline deployment: the IDS is deployed inline and analyses live traffic. De facto, it is an Intrusion Prevention System (IPS)
  Attacks can now be prevented



Host IDS (HIDS)

- Looks at traffic on the local host:
  - NIC in non-promiscuous mode
  - May also consider
    - Logs
    - System calls
    - Host activities
- IDS tuned for local services only

Distributed IDS (DIDS)

- Multiple Sensors send events to a centralised manager
- Sensors collect events
- NIDS and/or HIDS
- Manager correlates collected events
- Use a dedicated network or VPN for Probe-Manager traffic
- Have evolved towards that is commercially known as: **S**ecurity **I**nformation and **E**vent **M**anagement (**SIEM**)

How an IDS works

Input information

- Application-specific information: correct data flow, etc,...
- Host-specific information: local logs, syscalls, file system changes.
- Network-specific information: packets, etc,...

Intrusion detection policies

- Known-good: alert anything out of usual
  - Anomaly detection
- Known-bad: database with known attacks or attackers
  - Reputation-based detection
  - Signature-based detection

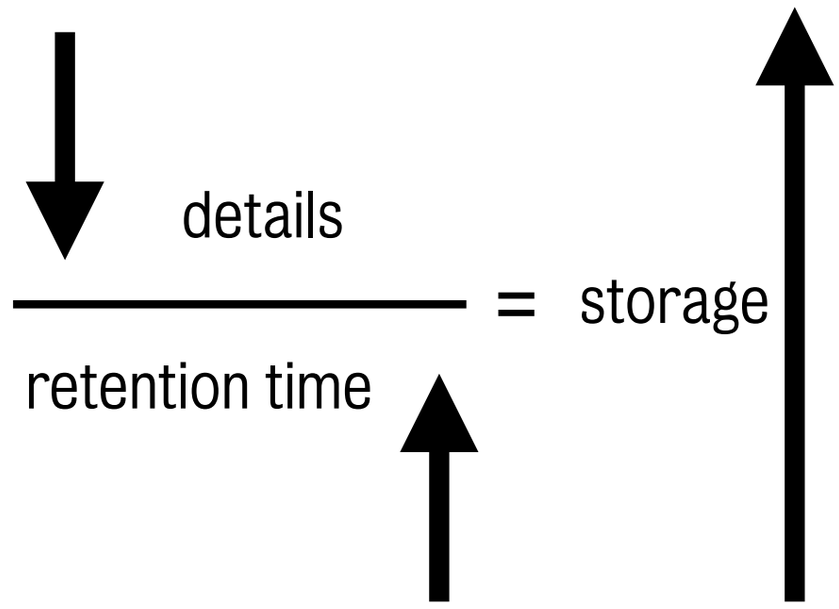
Response on intrusions

- Passive response
- Active response

Attack analysis

Data collection

- Collected data:
  - Alert data: IDS alerts
  - Log data: complete host logs
  - Statistical data: network stats
  - Session data: 5-tuple flows
  - Packet string data: e.g., HTTP headers
  - Full packet capture: PCAP files
    - Maybe only packet headers (64 bytes)
- Tools:
  - Packet capture: tcpdump, dumpcap
  - Session data: netflow, IPFIX
  - Session string: URLsnarf
  - Logs: syslog

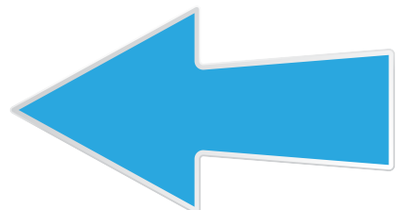


Network IDSs: SNORT

- Snort is an open source **real-time network based** intrusion detection system - based on **libcap**

- Simple rule-based analysis engine

- Pattern-matching capability



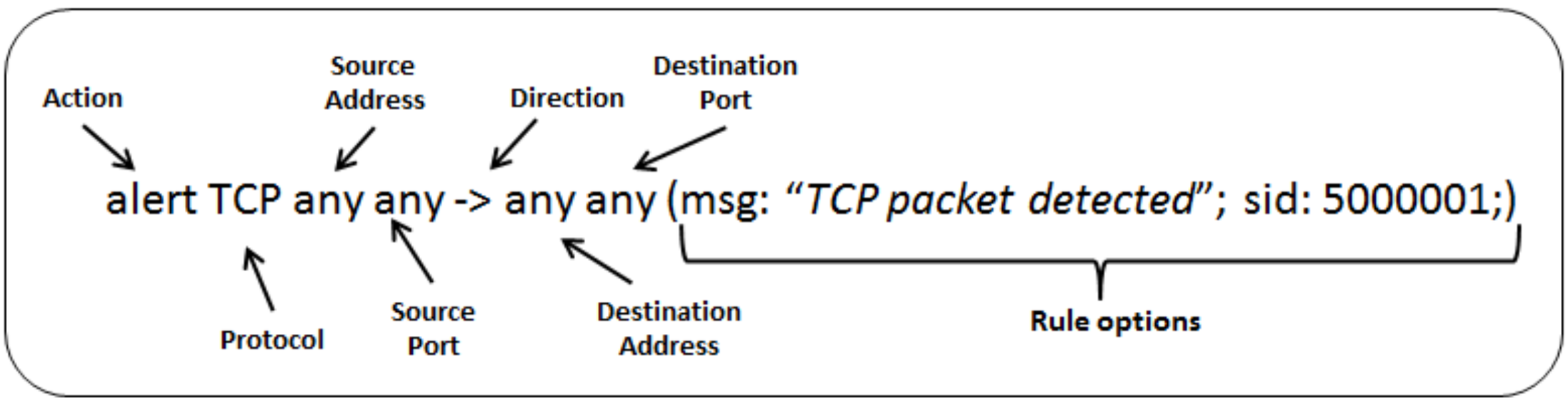
- Support from the open source community

- Signatures

- Plugins, extensions

Snort rules

- Snort rules are composed of:
  - HEADER: defines matching packets
    - Rule's action
    - Protocol
    - Source and destination IP addresses and netmasks
    - Source and destination ports
  - OPTIONS: defines content matching and additional functions



Problems with network IDSs

- They require a **mirror port** on a switch to be able to observe the entire network traffic

- **Visible problem**: if the network is partitioned (for example it has a DMZ) a separate IDS is required for each partition.

- **Vulnerable to evasion techniques**:
  - The sniffer logs also those packets that would be discarded by the operating system
  - Useless when encryption is used
  - The way packets are handled by the IDS and the end host might be different
  - Attackers could generate decoy attacks of perform very slow attacks

Evasion: insertion

- An IDS might accept a packet that the end system will reject.

The attacker sends a number of out-of order packets

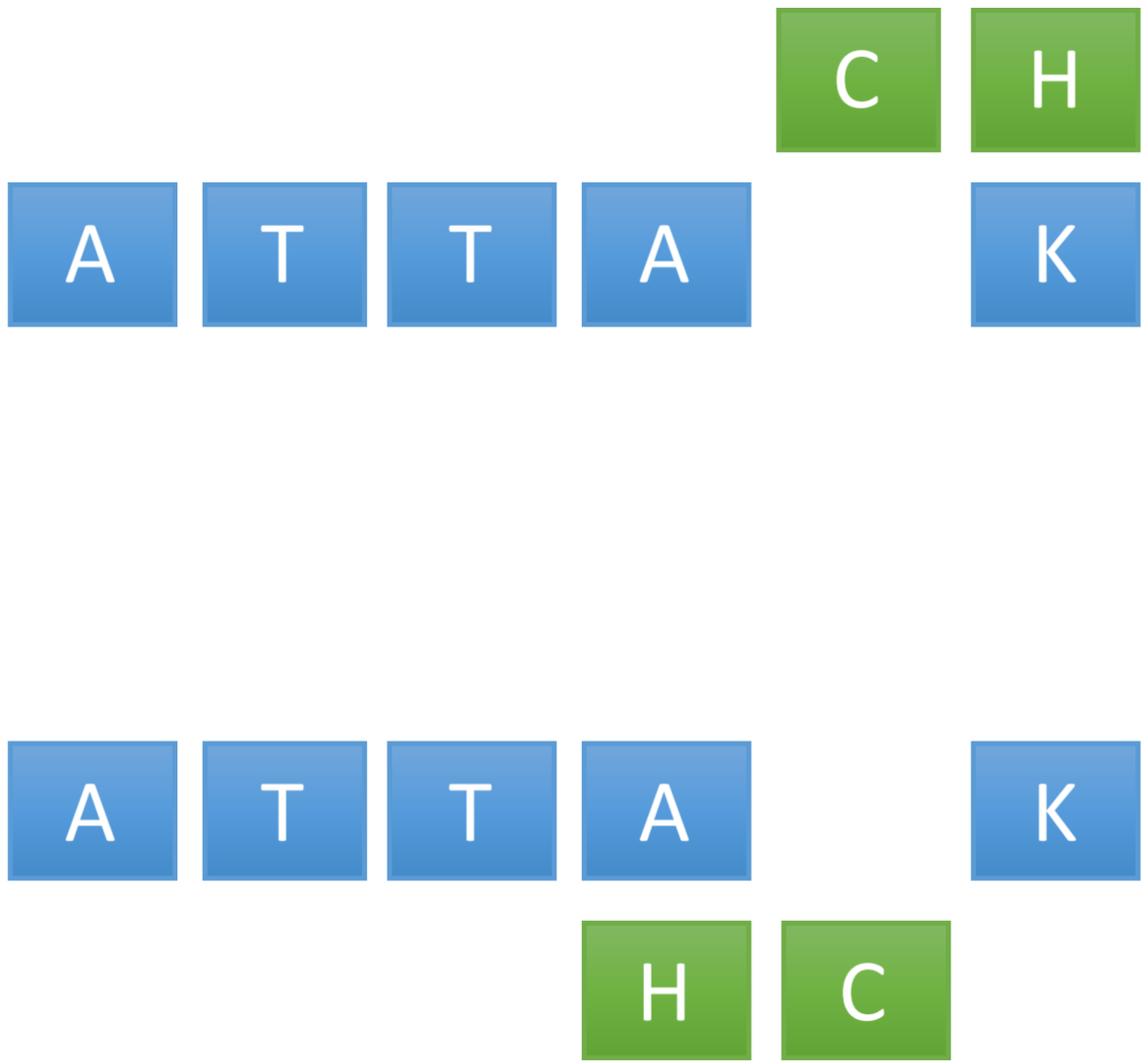
Malformed packet

The IDS is looking for the “ATTACK” signature, but accepts the malformed packet and is evaded

The end system discards the malformed packet, and the attack succeeds

Evasion: de-fragmenting behaviour

- What happens if two TCP segments overlap?
  - Most system favour old data
  - Windows favours new data



Forward overlap

Reverse overlap

Evasion: other de-synchronization techniques

- The destination host may not accept TCP segments bearing certain options
- The destination host might drop packets with old timestamps
- The destination host may not check sequence numbers on RST packets

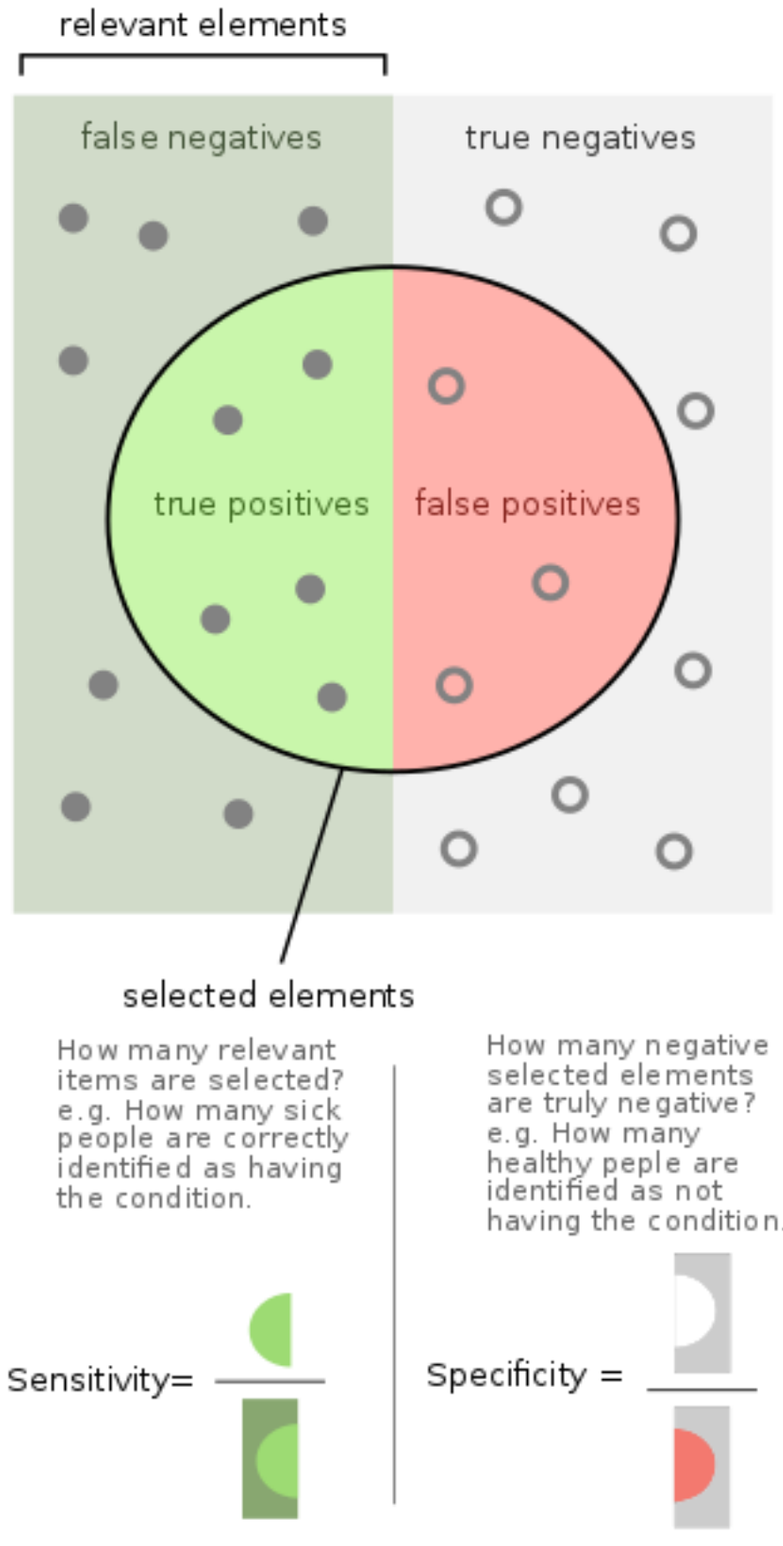
Partial solutions:

- Take into account the OSes of the target systems
- Take into account the installed services and their configuration
- Deploy a “normalizer” module that blocks malformed packets

Problem: IDSs should be easily deployable.

Measuring performance?

		True Condition	
	TOTAL	Condition positive	Condition Negative
Predicted condition	Predicted condition positive	**True Positive (TP)**	**False Positive (FP)**
	Predicted condition negative	**False Negative (FN)**	**True Negative (TR)**



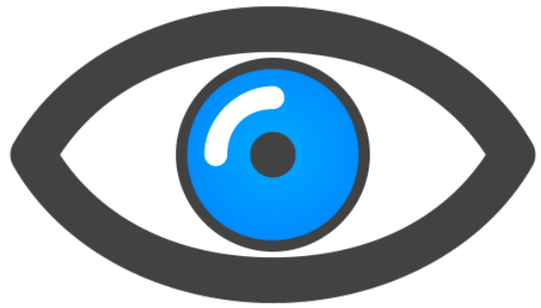
- Terminology:
  - Sensitivity, True positive rate (TPR), Recall, probability of detection
  - Specificity (SPC), Selectivity, True negative rate (TNR)
  - Accuracy = (TP + TN) / TOTAL
  - F1 score = 1/(1/Recall + 1/Precision)/2
  - ROC (Receiver Operating Characteristic Curve): Trade-offs between true positive (benefits) and false positive (costs)

Honeypots

Honeypots

Honeypots

- A honeypot is a trap set to
  - detect,
  - deflect,
  - or in some manner counteract



- ... attempts at unauthorised use of information/network (systems)

- Flexible tool with multiple applications:
  - Prevention
  - Detection
  - Information gathering

Value of honeypots

- Its value lies in the unauthorised or illicit use of the resource
  - Primary value is to collect information
  - They add little direct value to protecting the network

- It can be viewed as an intrusion detection technique used to
  - Learn from unknown attacks
  - Study intruders modus operandi
  - Better identify, understand and protect against threats

- Traffic landing in a honeypot is unsolicite

In practice

- Deployment
  - It is typically located in the DMZ or outside the boundary router
  - Virtual environment

- Goal
  - Look as real as possible
  - In-depth monitoring
  - Relevant to the attacker

Classification

- By level of interaction
  - High
  - Low
- By implementation
  - Virtual
  - Physical
- By purpose
  - Production
  - Research

Low interaction honeypots

- Limited interaction:
  - Emulates services, applications, and OS's
  - Cannot be exploited to get complete access to the honeypot
  - The attacker is limited to the level of emulation
- Advantages:
  - Low risk
  - Easy to deploy/maintain
- Disadvantages
  - They capture limited information

High interaction honeypots

- Real operating system and applications:
  - No emotion is used, attacker gain full access a net/sys

- Advantages:
  - Capture extensive information

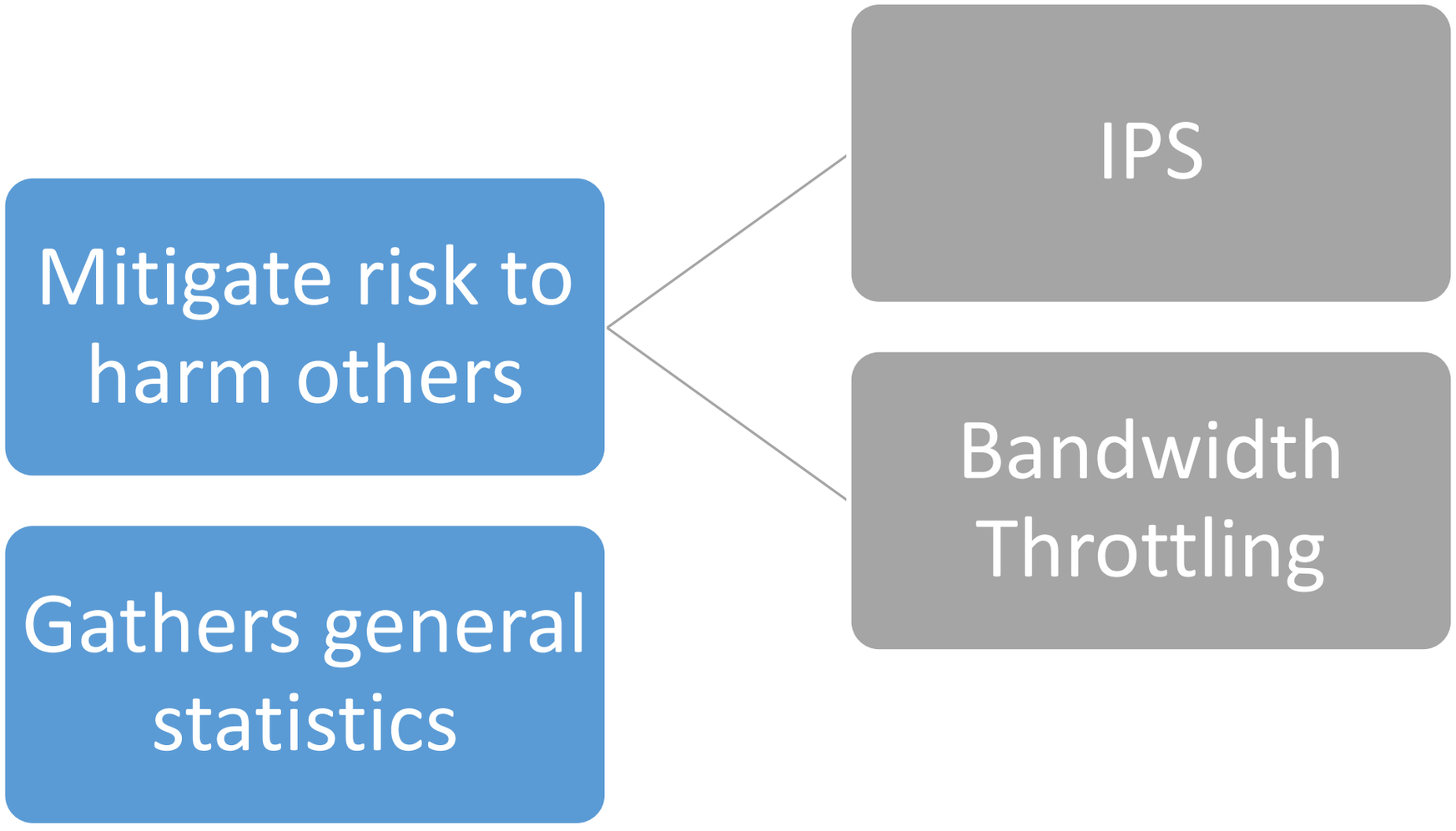
- Disadvantages:
  - High risk and time intensive to maintain

Common architectures

- Bests practices
  - A highly bastioned network
  - Every packet is kept

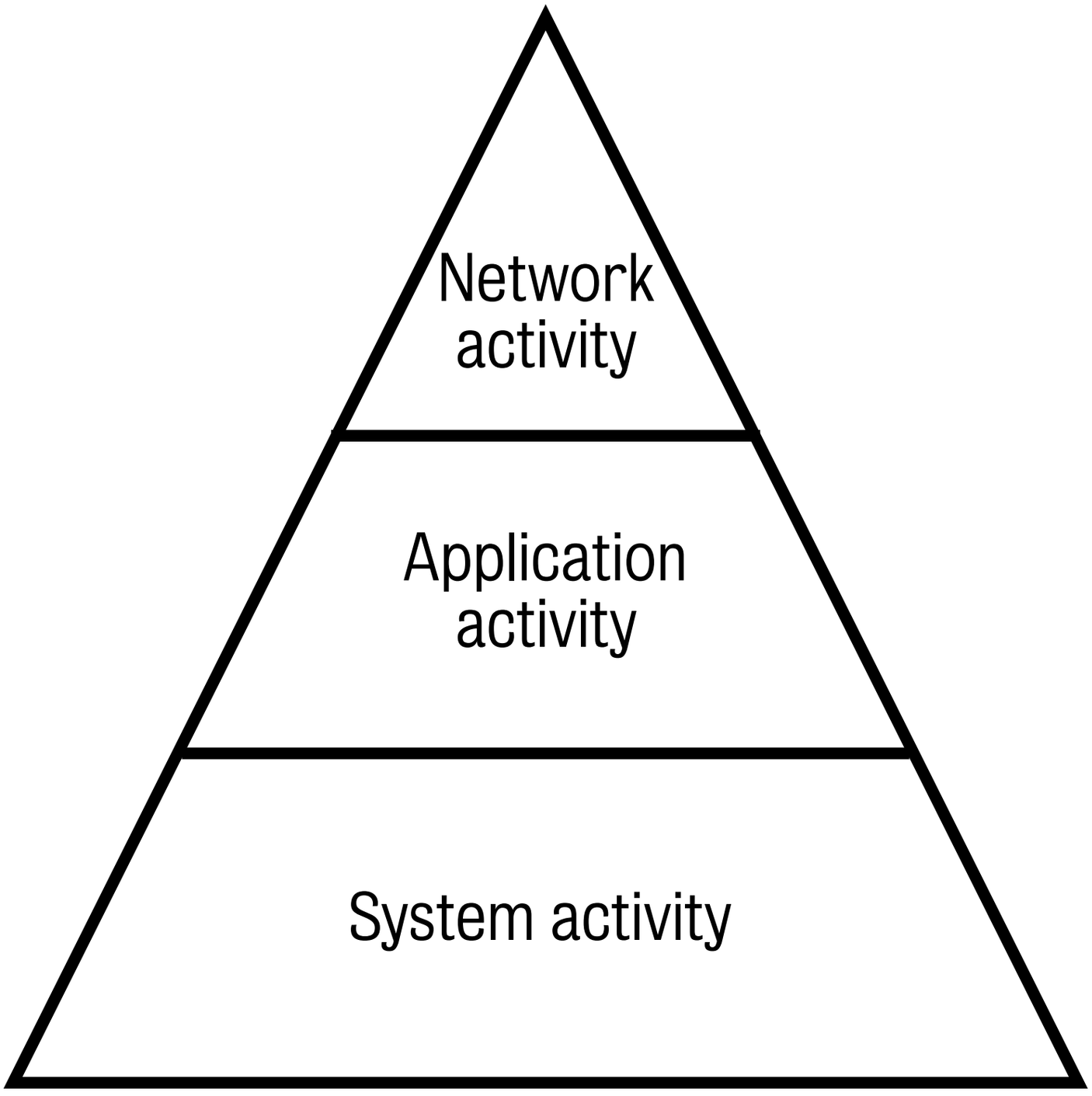
- Phases
  - Data control
  - Data capture
  - Data analysis

Phase: data control



Phase: data capture

- Keep it all at all levels



Phase: data analysis

- Human-driven analysis
  - Rely on automated tools to process the data
- Machine-driven analysis
  - Assume that network connection are either:
    - MALICIOUS
    - ANOMALOUS

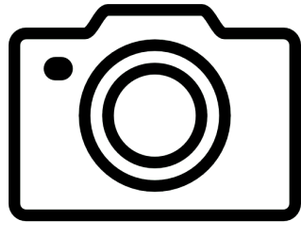
Case study: To Catch a Ratter

- "To catch a ratter: **Monitoring the behavior of amateur darkcomet rat operators in the wild.**" B. Farinholt et al. In *2017 38th IEEE Symposium on Security and Privacy (SP)*
- Type of malware analysed:
  - This malware has a hands-on operator interacting with each compromised machine
- Authors use a honeypot to:
  - Explore the motivation and behaviour of RAT (Remote Administration Tools) operators

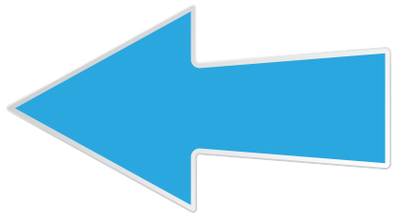
Typical RAT operations

- Capture audio from microphone

- Capture video from webcam



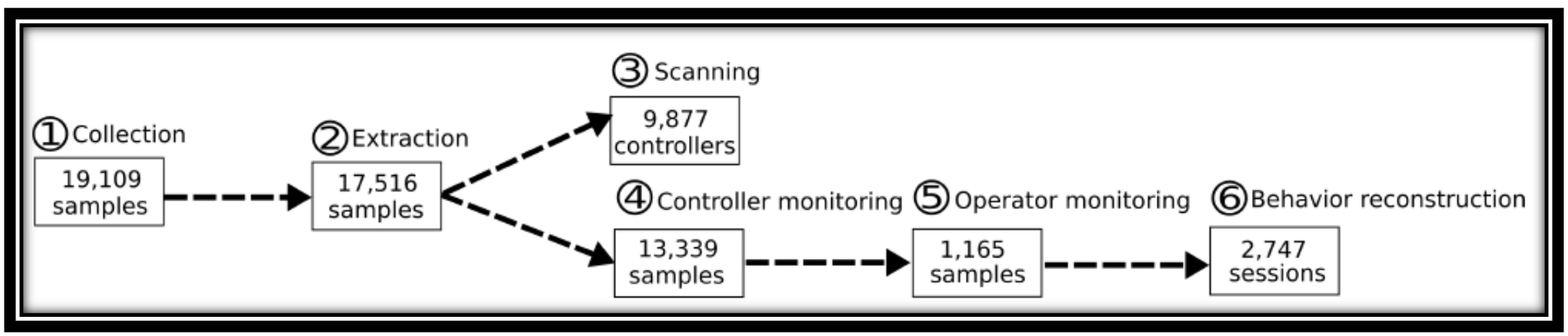
- Log keyboard input



- Browse files on machine

Methodology

1. Collection of DarkComet malware samples
    - Most popular sources are from Russia and Turkey.
2. Extraction
    - Password to decrypt network comms with the controller
    - Version of DarkComet
    - Campaign ID (affiliate ID from the operator)
    - Info about the controller:
        - Domain names, IP addresses, ports.
3. Extraction and controller monitoring (see paper)



Operator monitoring

Experiment 1	Experiment 2
20 honeypots ran concurrently	8 honeypots run concurrently
Identical honeypots with minimal cosmetic difference	• Unmodified windows installation • PC gamer (male) • Medical doctor (male) • U.S. political figure (male) • Acadeic researcher (male) • Bitcoin miner • College student (female) • Bank teller

Honeypot limitations:

- No webcam or microphone
- No responses to attacker-initiated chat, communication
- No keystrokes for key logger
- Network containment policy

Behaviour reconstruction

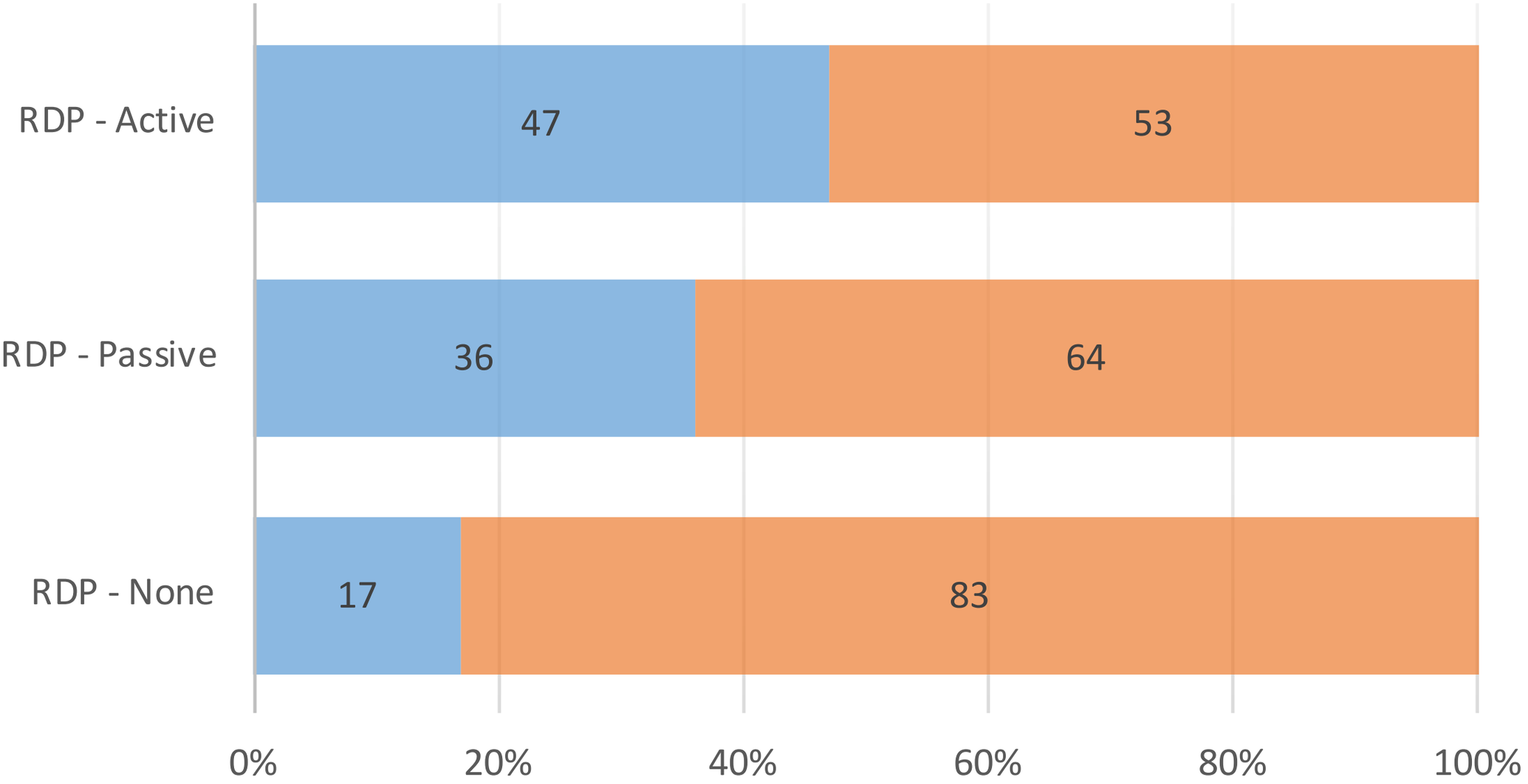
- Over the two experiments
  - 1165 samples
  - 2747 total sessions recorded
    - Reconstructed the network traffic
    - Analyze the operations that occurred
      - Capture screen (and timestamp)
        - Changes for Remote Desktop (**RDP**) sessions
      - 785 sessions
        - Resulted in engagement with the operator
      - Several week long experiment

Where operators came from?

	Global Scanning		*Live Trials*	
Country	*Cnt*	*Pct*	*Cnt*	*Pct*
Turkey	3,680	37%	222	25%
Russian Federation	1,495	15%	188	21%
United States	319	3%	36	4%
Brazil	306	3%	40	4%
France	283	2%	22	2%
Ukraine	282	2%	52	5%
Other	3,512	36%	307	35%
Total	9,877		867	

TABLE IV: Countries of the IP addresses of a) the global population of scanned DarkComet controllers, and b) the controllers to which our live trials connected, as resolved by MaxMind's GeoLiteCity database [38]. Addresses without resolution are omitted.

Interactivity



Operator actions

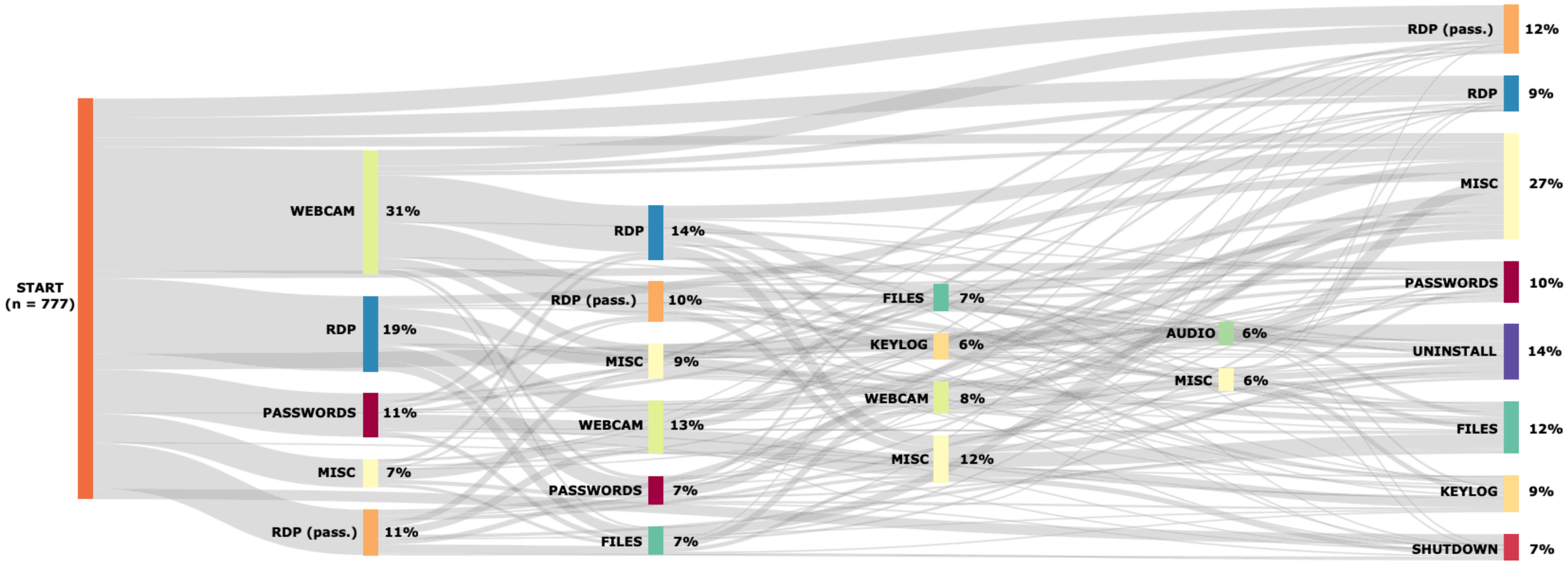


Fig. 5: Composite flowchart of prevalent operator behaviors and sequences broken down by RAT interaction phase and category. Individual paths are labeled with the percentage of all executions that traversed that edge. Sequences occurring in fewer than 5% of engaged executions are omitted. The figure shows an operator preference for engaging with remote desktop or surveillance first in a majority of trials. See Section IV-C for additional details.

Other type of honeypots

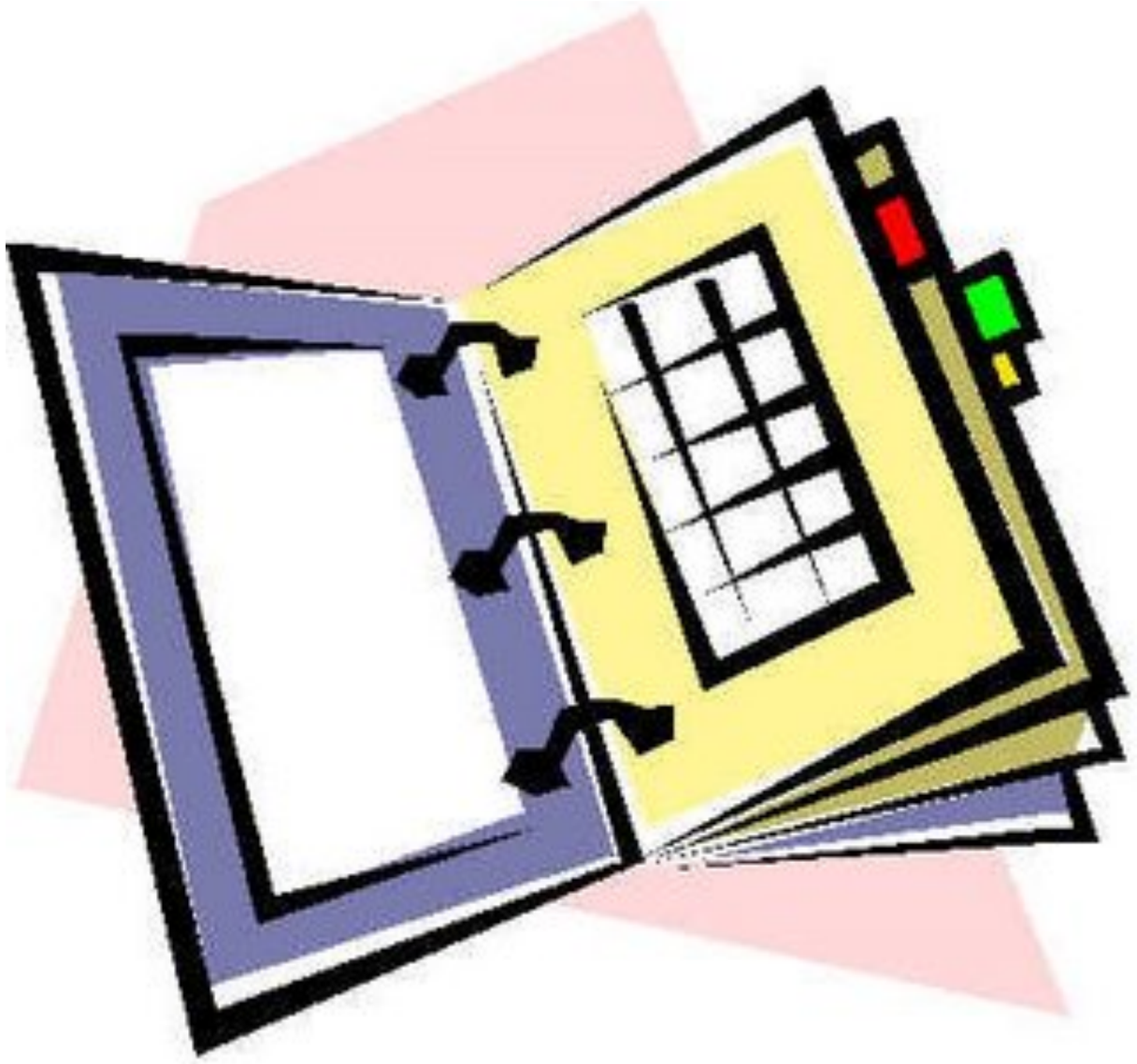
Honeytokens

- Honeypots that are not computer system
  - An unused email address
  - A fake database entry
  - etc,...

- Their value lies not in their use, but in their abuse

- Key idea
  - Their use is inherently suspicious
  - Necessarily malicious

Honeytokens: the first



Commons honeytokens

1. A bogus medical record called "John F. Kennedy" is created and loaded into the database. This medical record has no true value because there is no real patient with that name. Instead, the record is a honeytoken, an entity that has no authorized use. If any employee is looking for interesting patient data, this record will definitely stand out. If the employee attempts to access this record, you most likely have an employee violating patient privacy. It is as simple as that, no fancy algorithms, no signatures to update, no rules to configure. You load the records, monitor it, and if someone accesses it they most likely have violated the system's usage policy.

```
2.alert ip any any -> any any (msg:"Honeytoken
 Access - Potential Unauthorized Activity";
 content:"4356974837584710";)
```

Case study: Understanding the Use of Leaked Account Credentials

- What happens after you are pwnd: Understanding the use of leaked webmail credentials in the wild. Jeremiah Onaolapo, et al. In *Proceedings of the 2016 Internet Measurement Conference* (pp. 65-79). ACM.

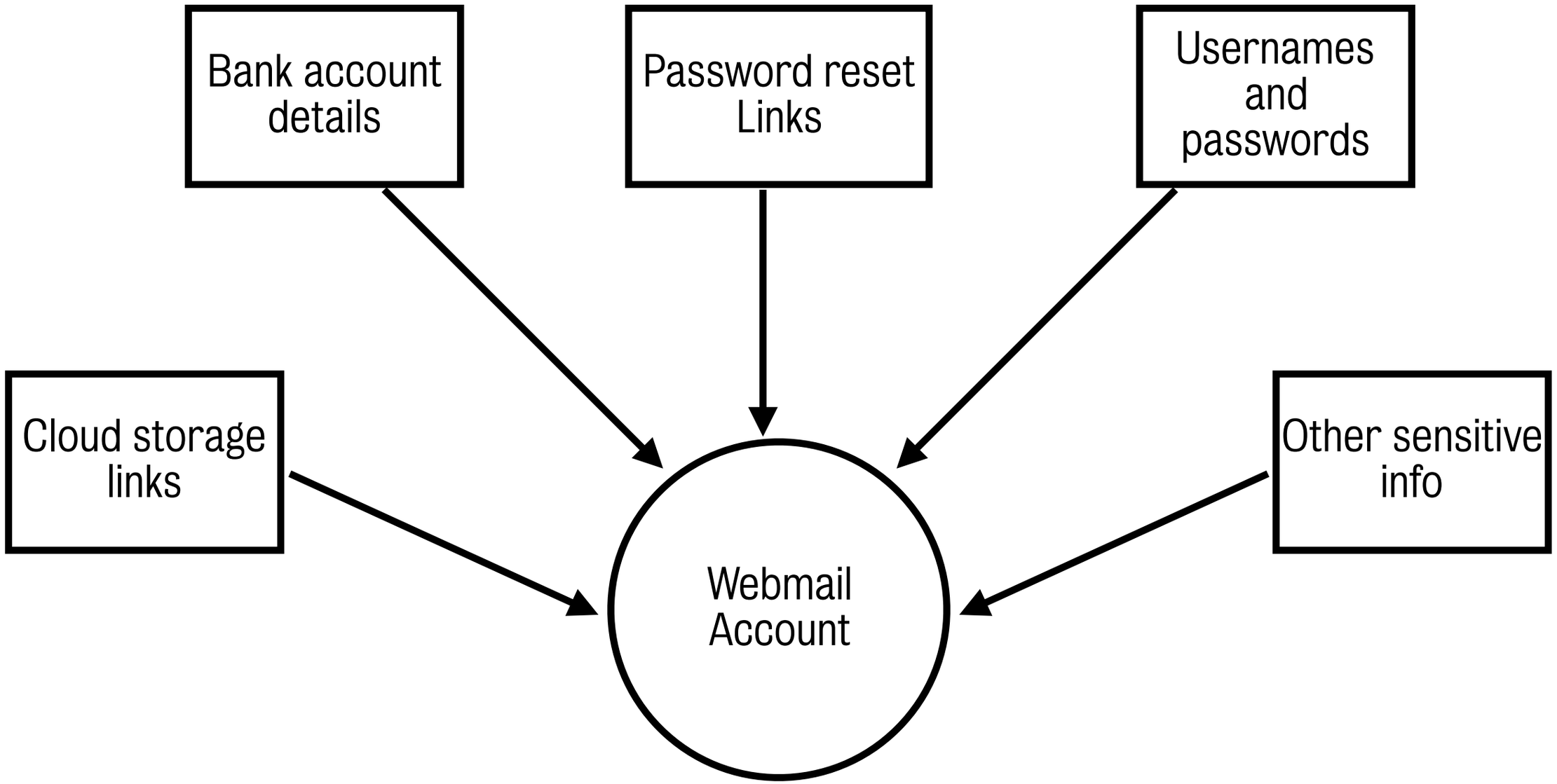
Case study: Architecture

1. Create and populate honey accounts
2. Configure monitor infrastructure
3. Leak Honeytokens
4. Record and analyse daya

Question

- What happens to online accounts **AFTER** they are compromised by criminals?
- Particularly interested in webmail accounts since they are often “hubs” that link other accounts

Web account “HUB”



Depths of the web

- Surface web
  - “anything that can be indexed by a typical search engine like Google, Bing or Yahoo”
- Deep web
  - “anything that a search engine can’t find”
    - e.g., government databases
- Dark web
  - “a small portion of the Deep Web that has been internationally hidden and is inaccessible through standard web browsers”
  - Most popular: TOR network via TOR browsers

Source - https://brightplanet.com/2014/03/clearing-confusion-deep-web-vs-dark-web/

Deeper questions

- What happens to webmail accounts after compromise
  - via the Surface Web?
  - via the Dark Web?

- Does language differentiation affect illegitimate accesses to webmail accounts?

- Three experiments

Honey accounts leaked via the surface web

Surface web study

- Created 100 Gmail honeypot accounts

- Populated them using the Enron corpus
  (The **Enron Corpus** is a large database of over 600,000 emails generated by 158 employees[1] of the Enron Corporation and acquired by the Federal Energy Regulatory Commission during its investigation after the company's collapse)

- Leaked account credentials via popular paste sites, underground forums, and malware, i.e., mimicked modus operandi of cybercriminals

- Collected and analysed data

Formats of leaks

```
Gmail accounts LeAkEd!!!

[username1]:[password1]
[username2]:[password2]
…
[username10]:[password10]
```

```
.:.gmail login.:.

[username11]:[password11]  16 May 1990  Luton, UK
[username12]:[password12]  22 Aug 1974  Uxbridge, UK
…
[username20]:[password20]  5 Dec 1975  Slough, UK
```

```
Gmail logins hacked by .:pHisH3R:.

[username21]:[password21]  16 Jun 1979  Chicago, IL
[username22]:[password22]  15 Mar 1970  Indianapolis, IN
…
[username30]:[password30]  5 Sep 1989  Wichita, KS
```

Honey accounts leaked via the Dark Web

Dark web study

- Used same infrastructure described previously
- Created 100 fresh honey accounts
- Populated them using the Enron corpus

Dark web study

- Leaked account credentials via hidden paste sites, underground forums, and black market

- No leak through malware

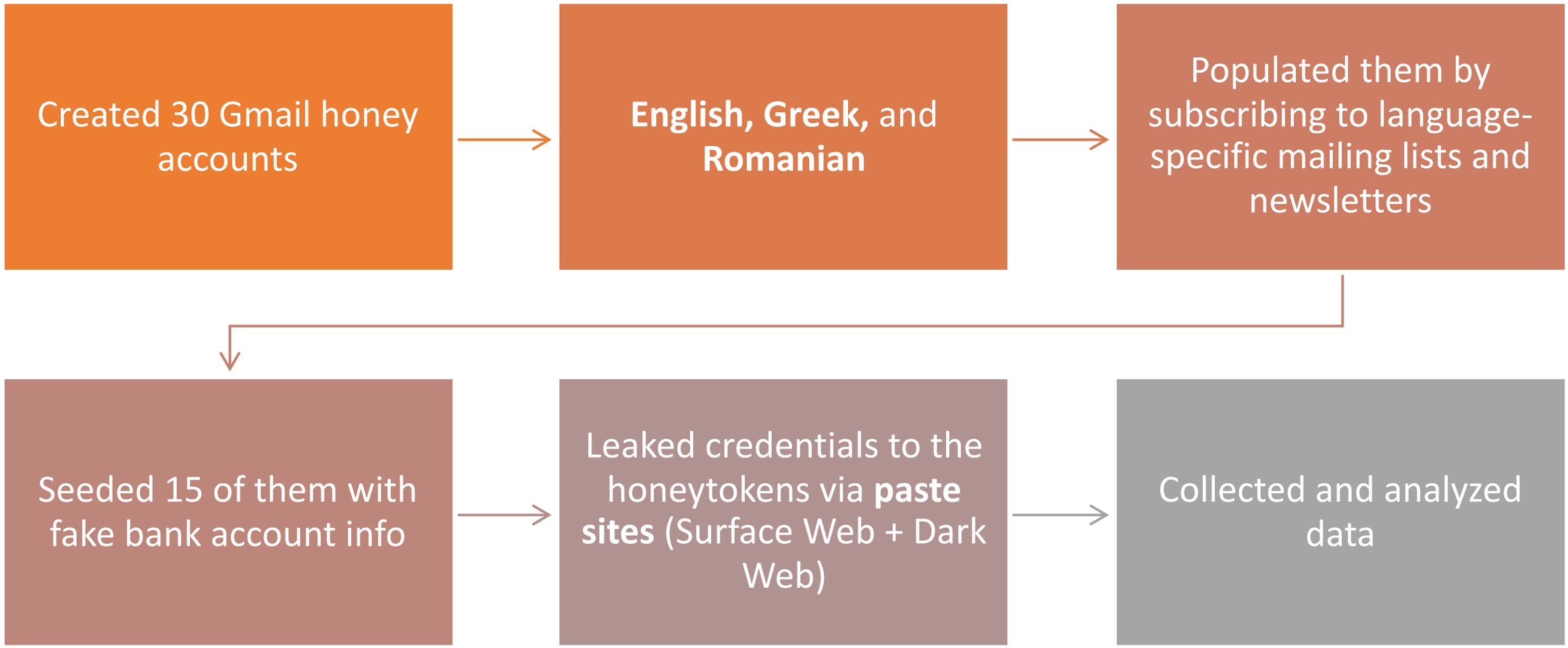
- Collected and analysed data

Historical example of black market – Silk Road
https://www.wired.com/2015/04/silk-road-1/

Babel in Honeytoken (The effect of Language Differentiation)

Language differentiation study

- Does language differentiation affect illegitimate accesses to webmail accounts?



Key findings

1

Many more accesses to honey accounts originated from the **Dark Web** than the **Surface Web**

2

Location (especially UK) and language differentiation **affect accesses** to honey accounts

3

However, results do not necessarily reflect what happens in all compromised webmail or online accounts

Challenges

- Finding actionable deviations
  - Normal behaviour
  - Attacker behaviour

- Intrusion events are not binary
  - Maximise your changes of being lucky
  - False positive fallacy
    - Noise vs Attack

- Turning events into actionable alerts
  - Use intelligence

- How do we get to learn about new threats
  - Honeypots
  - Human analysis

RECAP: What have we learnt?

- Firewalls are a type of intrusion prevention system
- Except that they don't typically have the ability to block know attacks. Instead, they rely on policies of expected behaviors
- They complement each other

- There are many depending on the type of classification
- For example, type of detection?

- Attacks are complex, this is a joint effort

- Know how they work? E.g., De-fragmenting attacks

- This is not a rigid concept. E.g., honeytokens

LAB time (EPISODE 5)

- Firewalls
- Brief about IPTables