To Catch a Ratter:

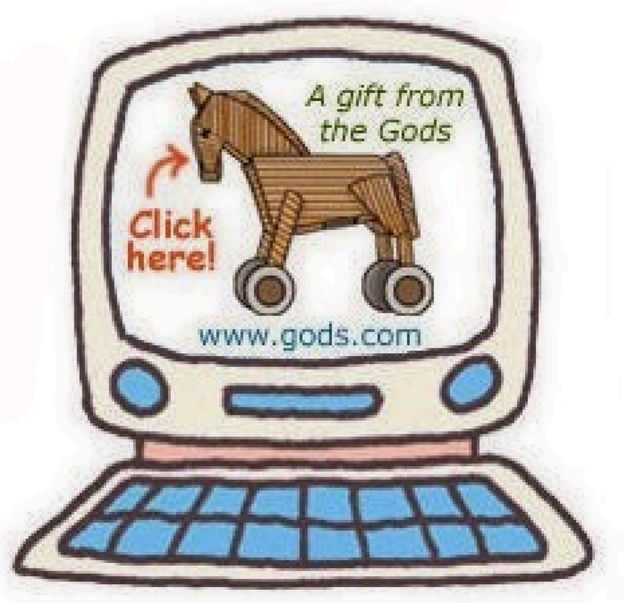
Monitoring the Behavior of Amateur DarkComet RAT Operators in the Wild

Brown Farinholt, Haikuo Yin, Kirill Levchenko — UC San Diego
Mohammad Rezaeirad — George Mason University
Paul Pearce — UC Berkeley
Hitesh Dharmdasani — Informant Networks
Stevens Le Blond — EPFL & MPI-SWS
Damon McCoy — New York University

Credit: https://2.bp.blogspot.com/-AEfsciiO6ig/UzmUYteaQ8I/AAAAAAAAa7o/pQTAm5m0rjw/s1600/Remote-access-Trojan-njRAT.jpg

Remote Access Trojans

- Let attackers control infected machines remotely
- Do not have exploits
- Operated **manually** vs. scripted malware
    - Ransomware, botnets are automated
    - RAT infections controlled by **human operator**



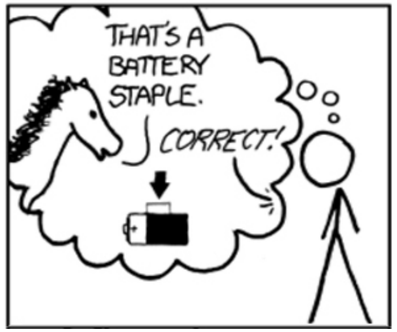
Capabilities

Webcam &
Microphone

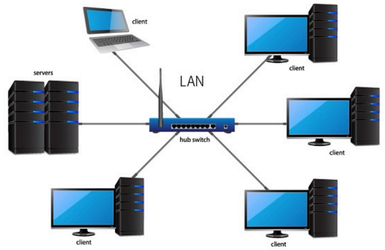
Chat Client

Remote Desktop

Filesystem



Passwords & Keylogger



Network Interrogation & Attack

Low Barrier to Entry

Availability: YouTube

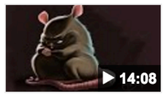
How to setup Dark Comet RAT (with download and pictures) : hacking
https://www.reddit.com/r/.../how_to_setup_**dark_comet**_rat_with_download_and/
Jul 10, 2014 - This is an tutorial on how to setup one of the best free rats, **dark comet**. First off download **dark comet** here: http://ge.tt/5jnRAPF2/v/0 ...

How to Download and Use DarkComet 5.3.1 - YouTube


https://www.youtube.com/watch?v=VdbFYAVKoDw
Mar 12, 2013 - Uploaded by N3rdizzle
LINKS: **DarkComet** 5.3.1: http://www.mediafire.com/?emhkqegn7774i4o Sandboxie: http://www.sandboxie.com ...

How to Download and Use DarkComet 5 3 1 (2016 updated) - YouTube


https://www.youtube.com/watch?v=58kSMFolNYs
Feb 11, 2016 - Uploaded by No Name
(UPDATED 2016-10-06) **DarkComet** 5.3.1: http://www.mediafire.com/file/84sxnqfh1c78wy5/DarkComet_5.3.1 ...

How To Setup DarkComet R.A.T Be Succesful With it - YouTube


https://www.youtube.com/watch?v=s7l-_lzRg5E
Nov 2, 2015 - Uploaded by imSoGettingBANNED
its clean -_- let me know when all the links eventually go down. **DarkComet**- https ://mega.nz/#!eIBC3LQB!

Setup a DarkComet RAT correctly [Tutorial] [Download] [No-IP] [2015 ...


https://www.youtube.com/watch?v=REVWH5F9PSg
Feb 17, 2015 - Uploaded by PreHacks
Download: http://adf.ly/132dOk FUD Crypter: https://www.youtube.com/watch?v=bJosUbPgU7c Open ...

Community: Dedicated Hacking Forums

Widespread Usage

Widespread Usage

Voyeurism

- School-issued laptop webcams
- Black market for webcam access

Widespread Usage

Voyeurism

- School-issued laptop webcams
- Black market for webcam access

Sextortion & Blackmail

- *Black Mirror*: “Shut Up and Dance”
- Miss Teen USA

Widespread Usage

Voyeurism

- School-issued laptop webcams
- Black market for webcam access

Sextortion & Blackmail

- *Black Mirror*: “Shut Up and Dance”
- Miss Teen USA

Surveillance & Espionage

- Syria DarkComet Skype tool

Widespread Usage

Voyeurism

- School-issued laptop webcams
- Black market for webcam access

Sextortion & Blackmail

- *Black Mirror*: “Shut Up and Dance”
- Miss Teen USA

Surveillance & Espionage

- Syria DarkComet Skype tool

- Attacks can be targeted…
- But many attackers seek large numbers of victims
  - Spread online (download links, cracked software)
- **Common Theme: Accessing victim user**

Research Questions & Motivation

Research Questions & Motivation

What do RAT operators do with compromised machines?

Research Questions & Motivation

What do RAT operators do with compromised machines?

Goal: To understand common use patterns of RATs in the wild (at scale)

- RATs used criminally, cause harm
- Elicit attacker methods, motivations
- Evaluate potential defenses
- Generally understand their use cases

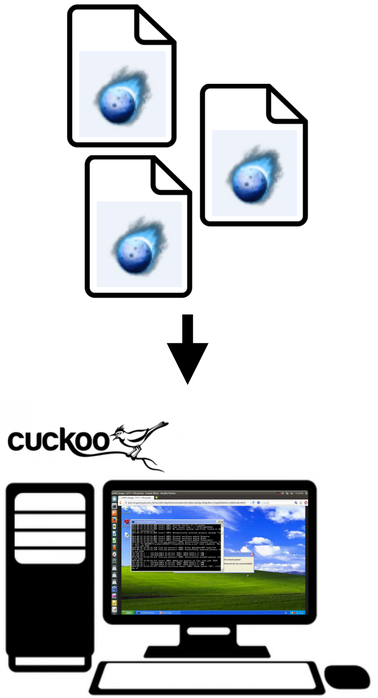
The Plan

The Plan

- Acquired **DarkComet RAT samples** from VirusTotal

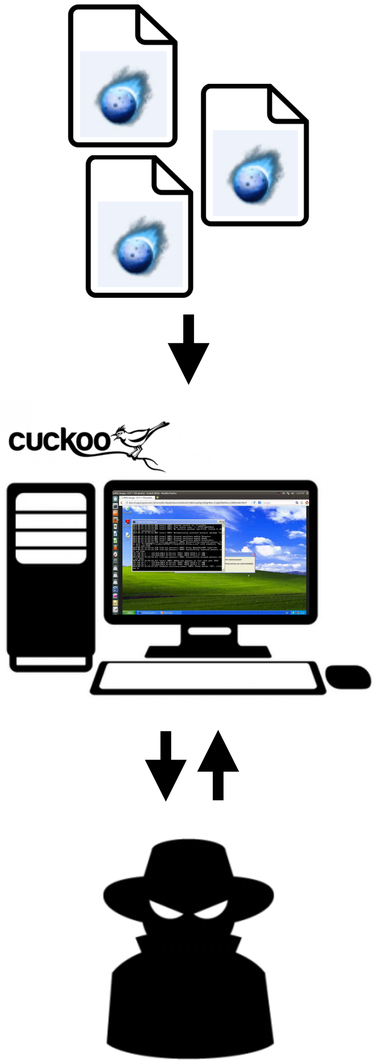
The Plan

- Acquired **DarkComet RAT samples** from VirusTotal
- Executed them in malware sandbox **honeypots**



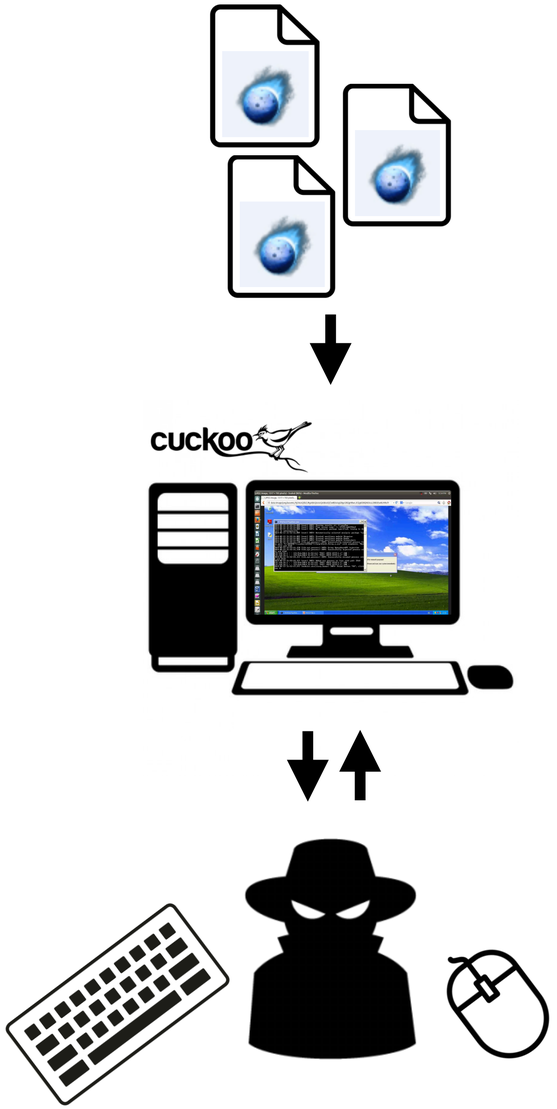
The Plan

- Acquired **DarkComet RAT samples** from VirusTotal
- Executed them in malware sandbox **honeypots**
- Recorded **network traces** of operator interaction



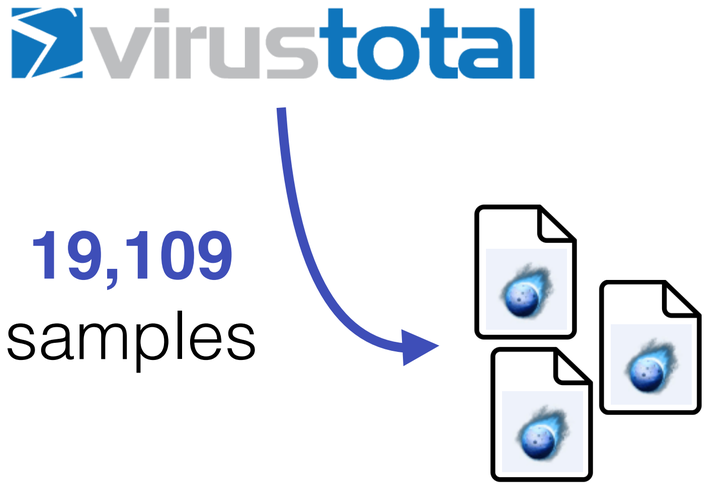
The Plan

- Acquired **DarkComet RAT samples** from VirusTotal
- Executed them in malware sandbox **honeypots**
- Recorded **network traces** of operator interaction
- Decrypted to obtain **operator command** sequences

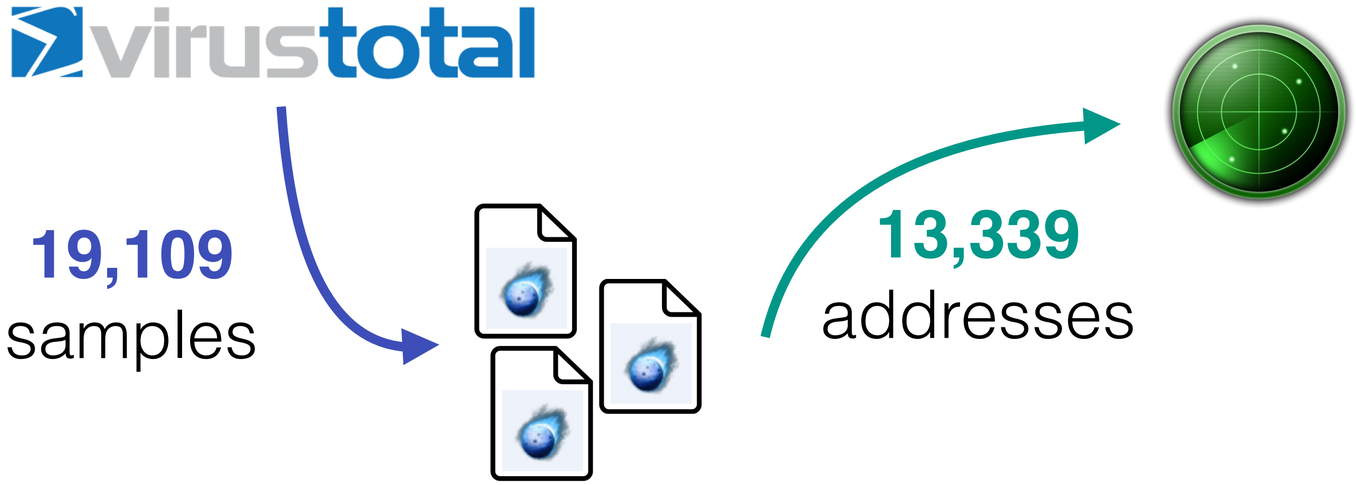


Experiment

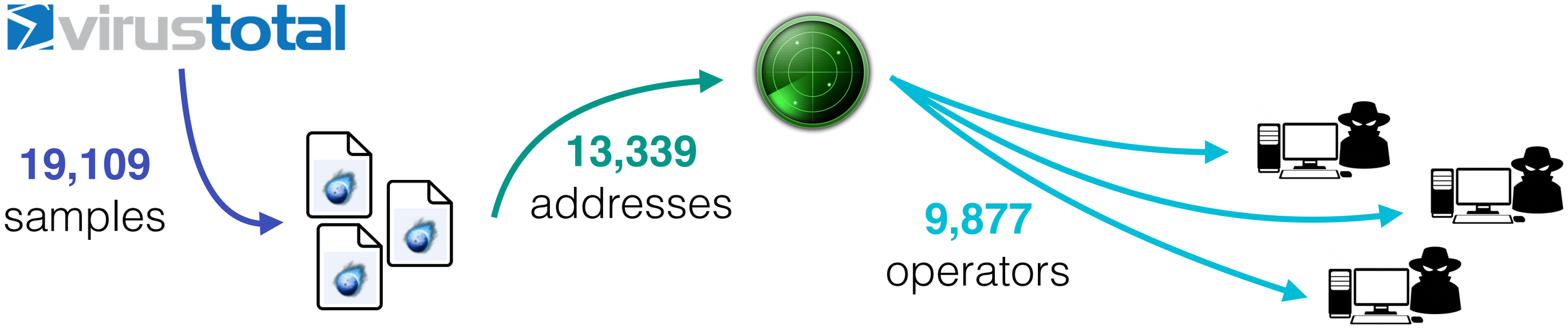
Experiment



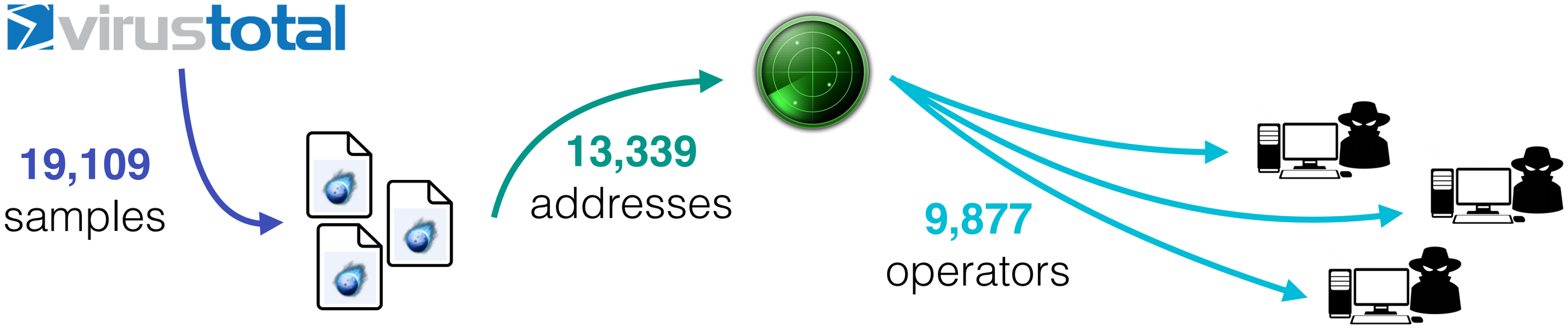
Experiment



Experiment

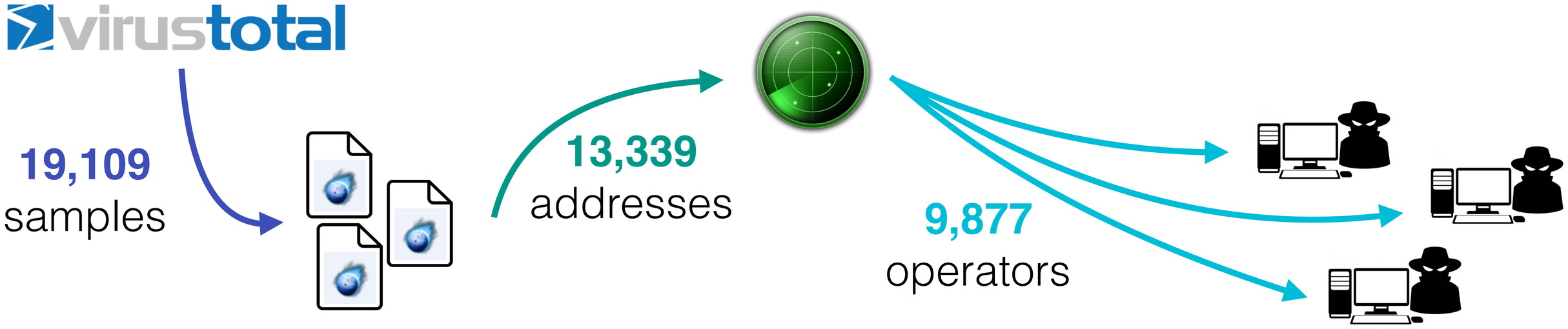


Experiment

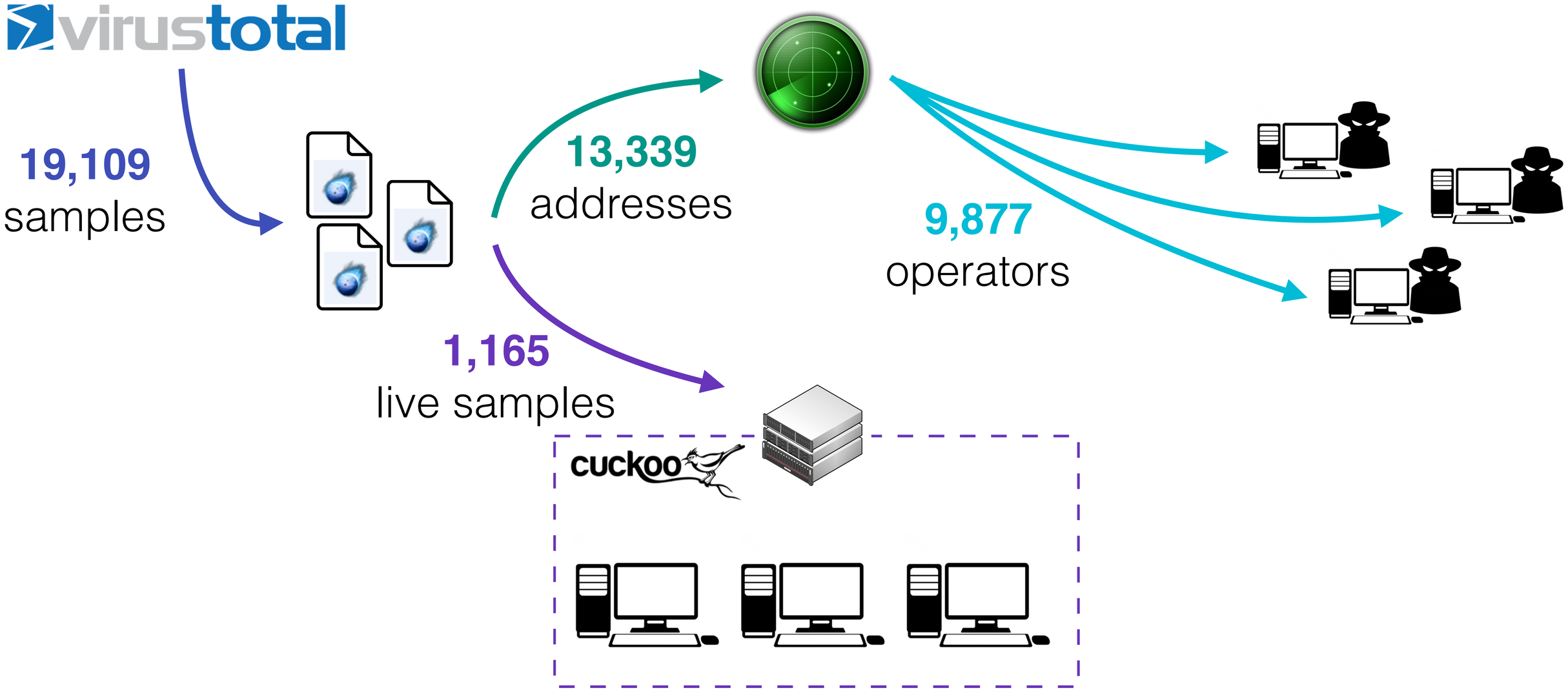


- 89% residential IPs
- 37% Turkish (#1)
- 15% Russian (#2)
- Diurnal liveness pattern

Experiment



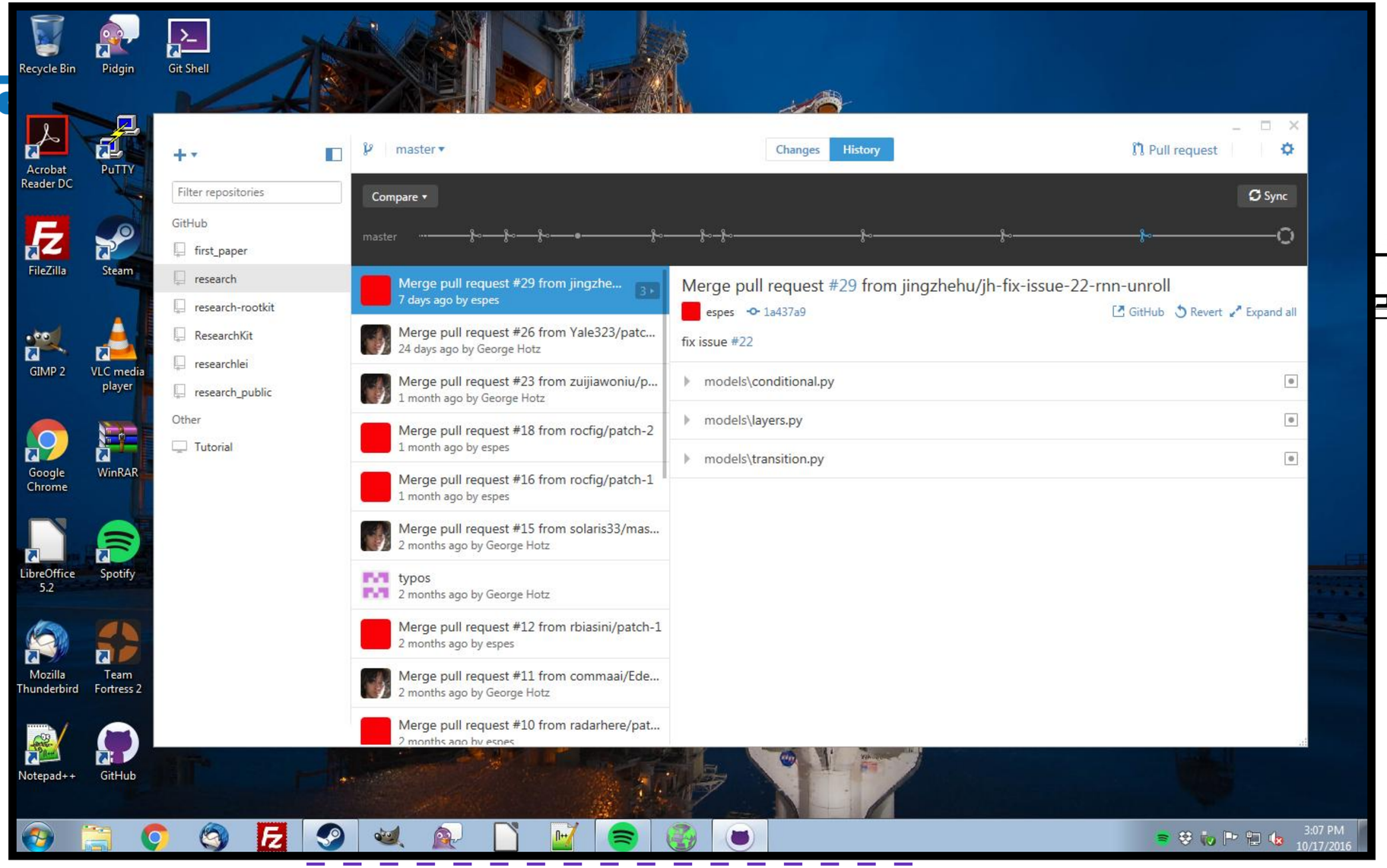
Experiment


virustotal
19,109
samples
13,339
addresses
9,877
operators
1,165
live samples
cuckoo

Experiment

virustotal

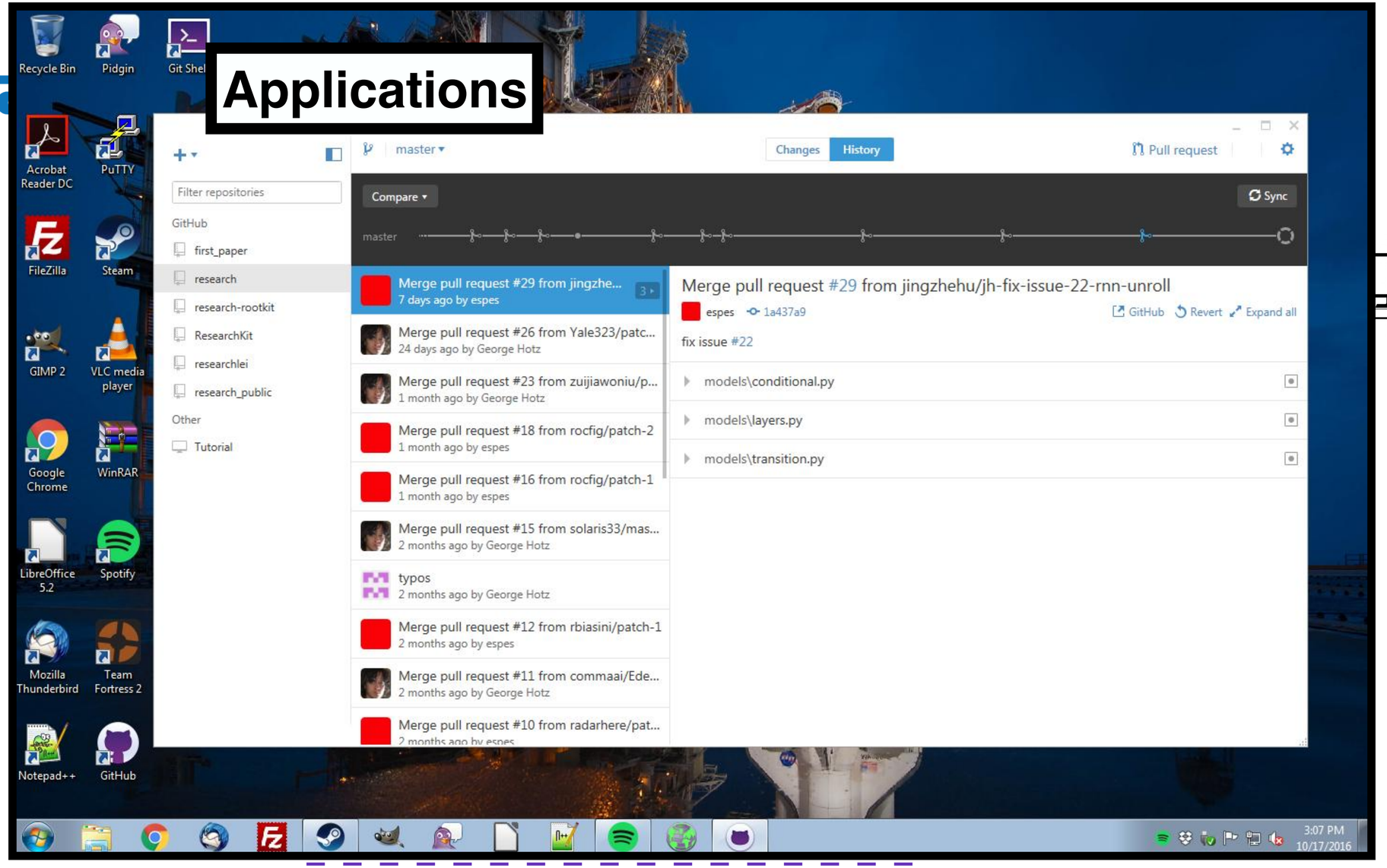
19,109
samples



Experiment

virustotal

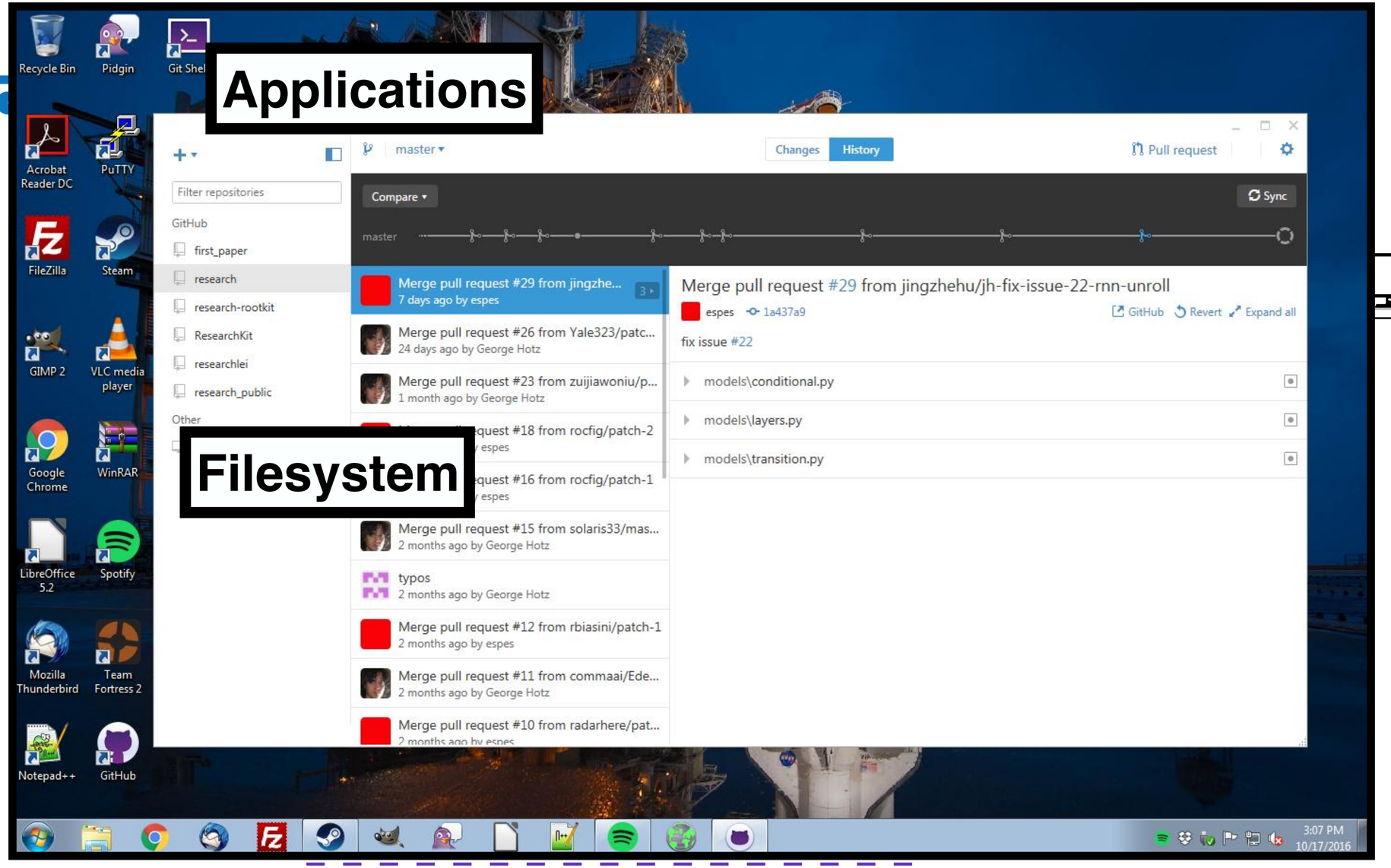
19,109
samples



Experiment

virustotal

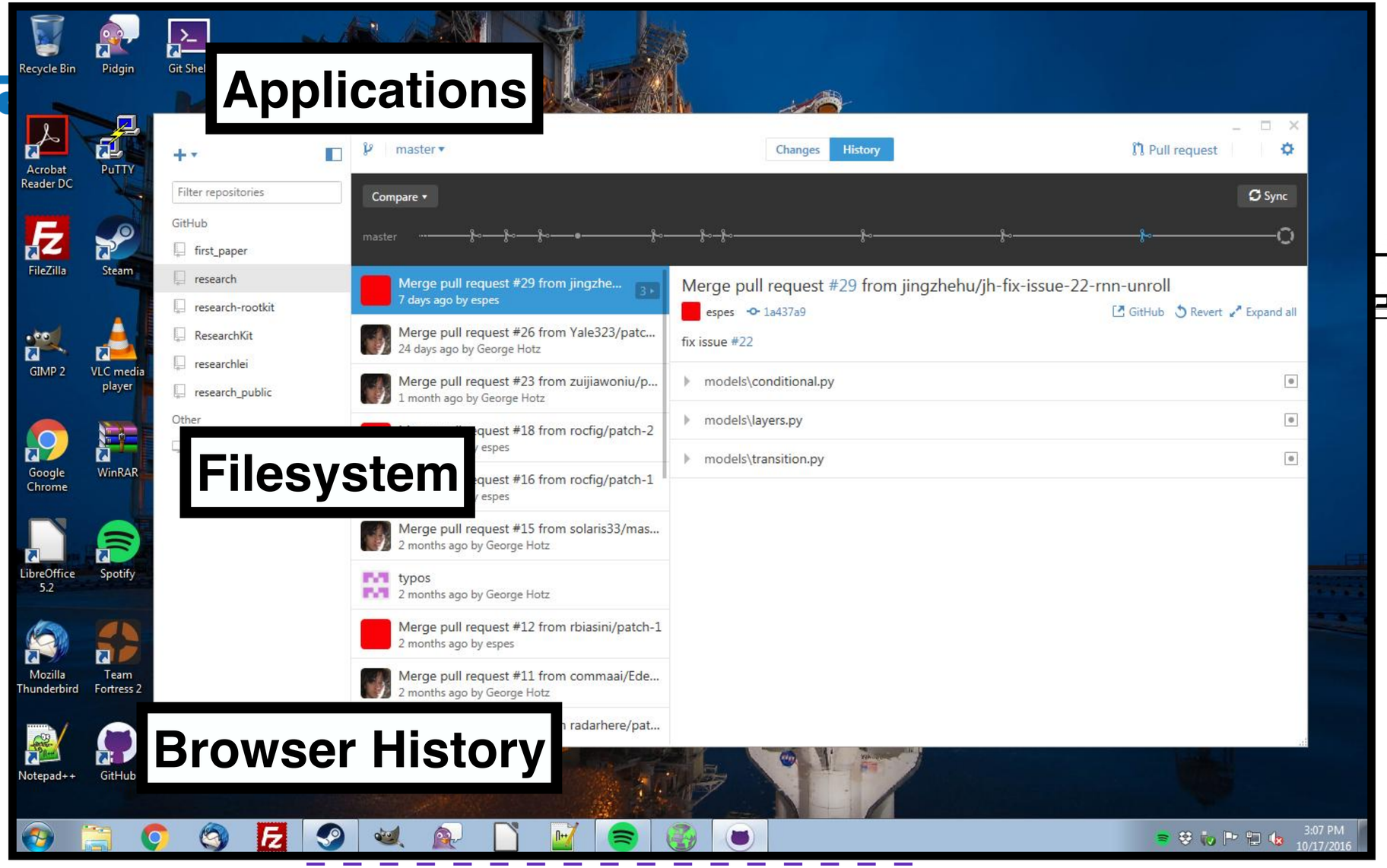
19,109 samples



Experiment

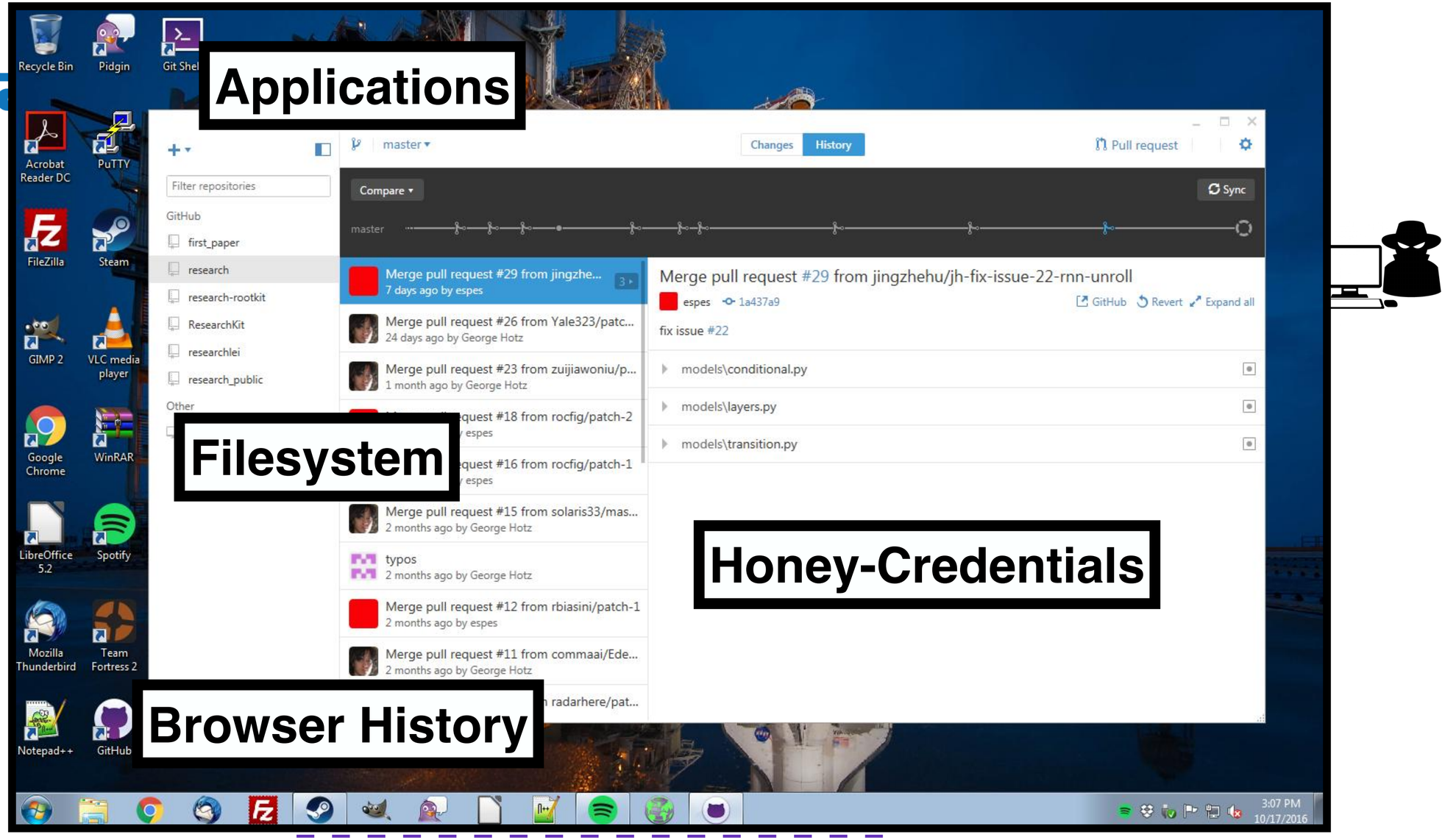
virustotal

19,109 samples

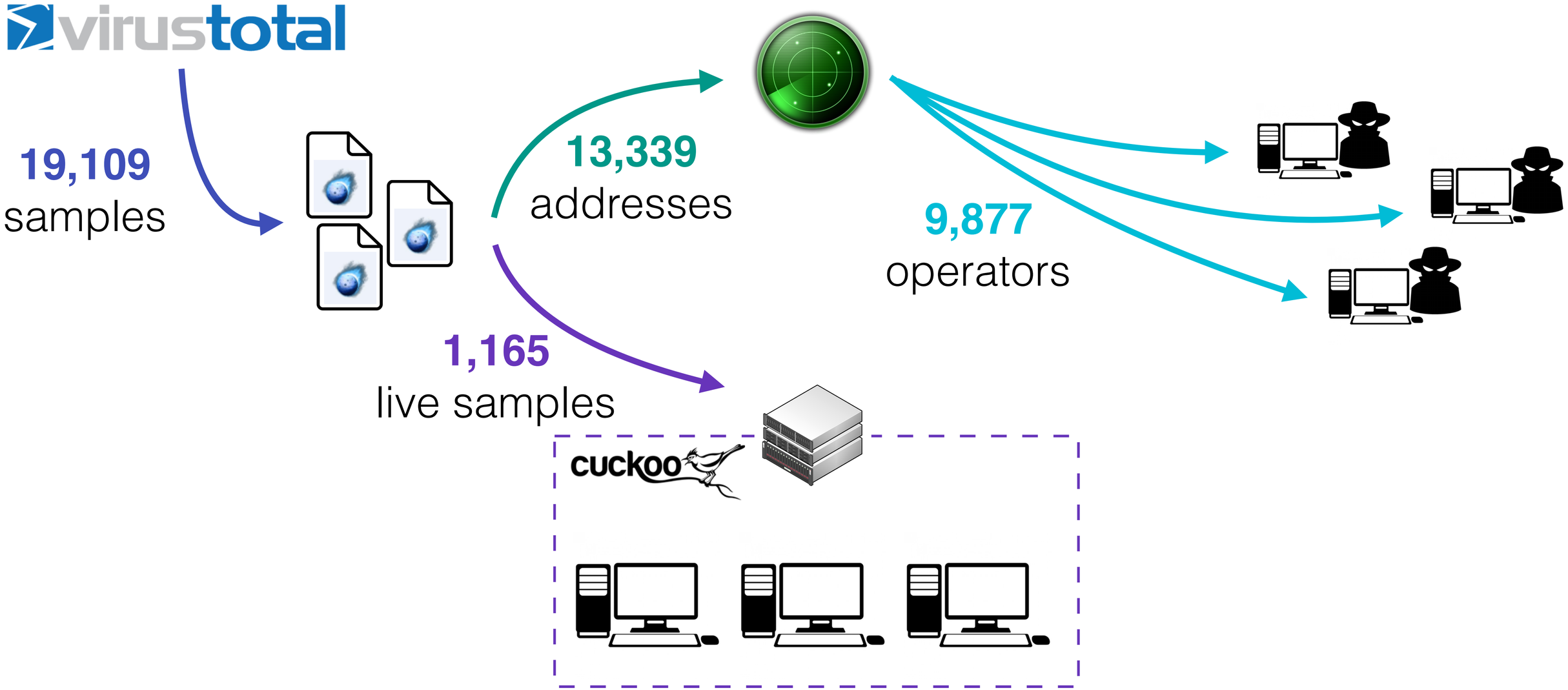


Experiment

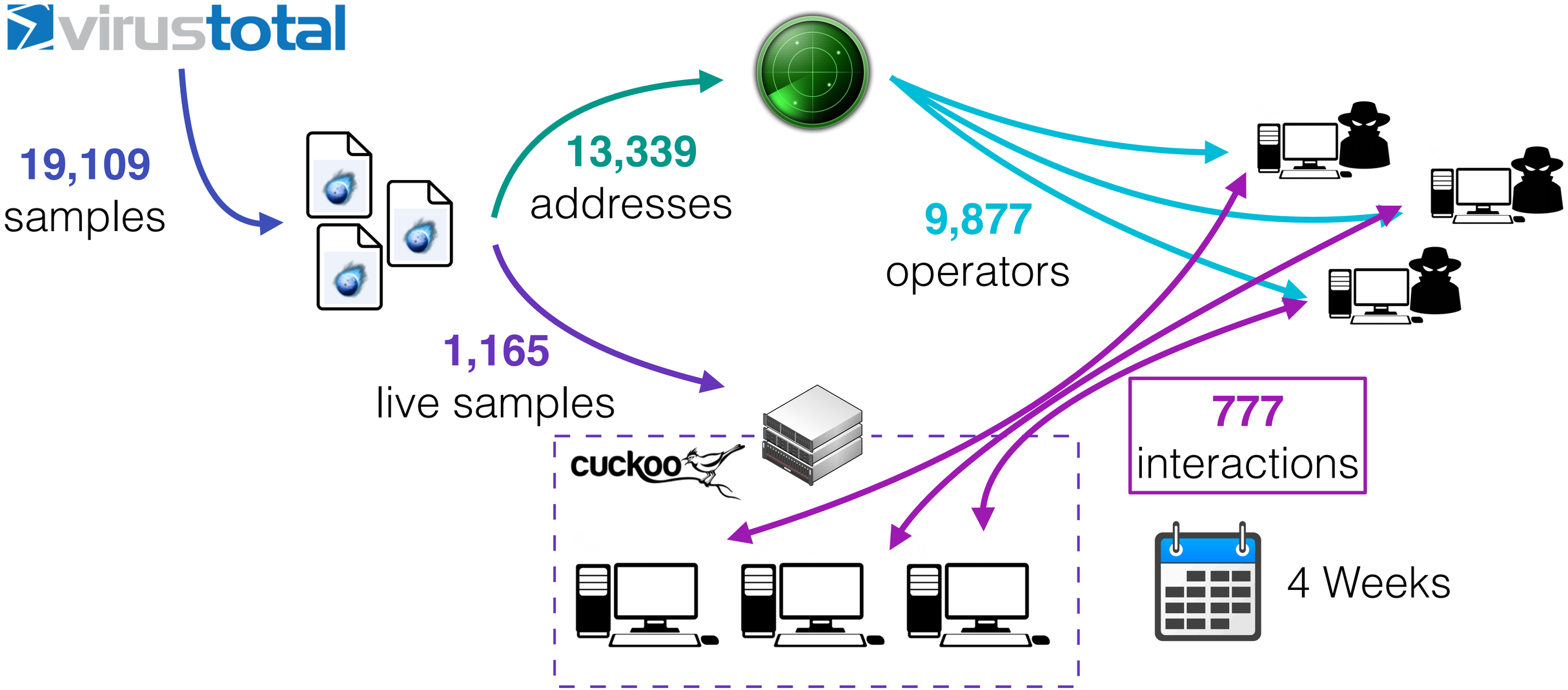
19,109
samples



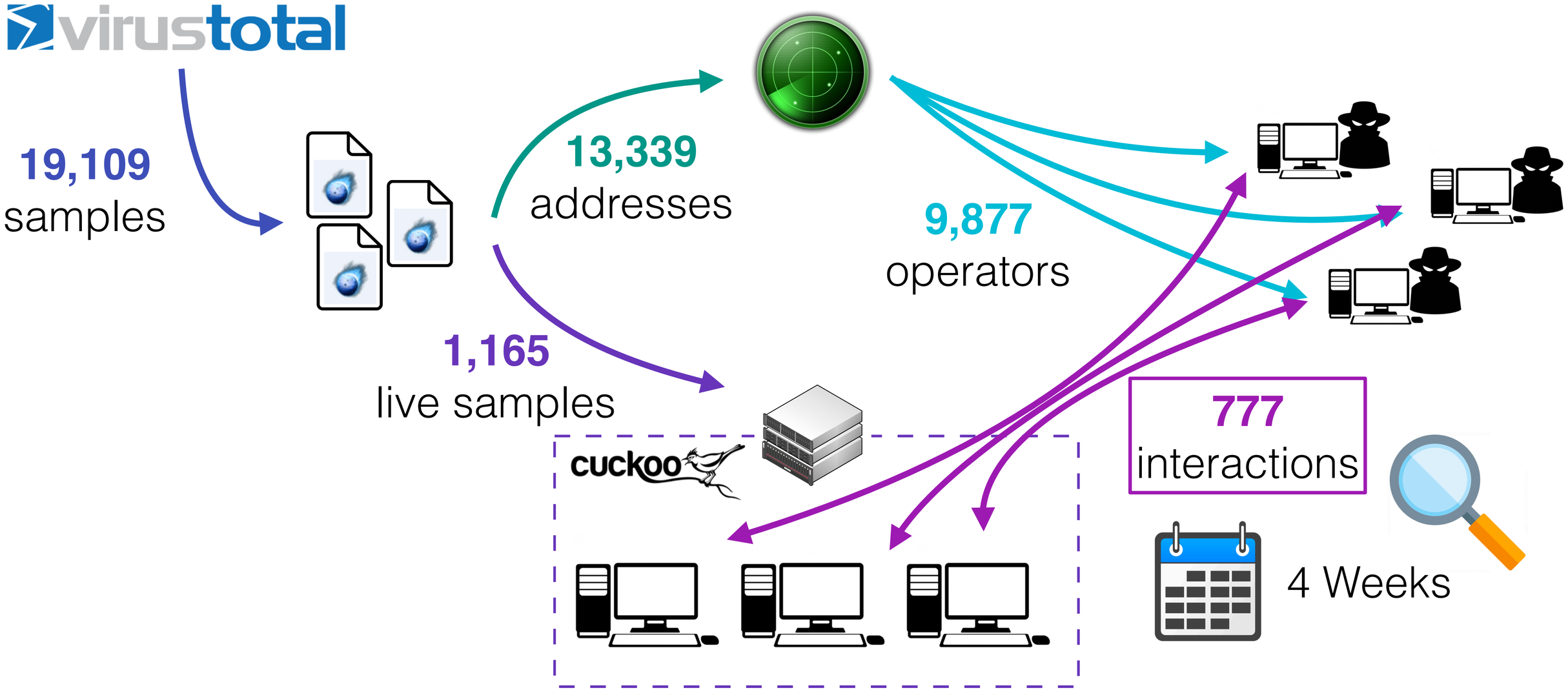
Experiment


virustotal
19,109
samples
13,339
addresses
9,877
operators
1,165
live samples
cuckoo

Experiment


virustotal
19,109
samples
13,339
addresses
9,877
operators
1,165
live samples
cuckoo
777
interactions
4 Weeks

Experiment


virustotal
19,109
samples
13,339
addresses
9,877
operators
1,165
live samples
cuckoo
777
interactions
4 Weeks

Experimental Biases

Experimental Biases

Targeted Attacks

We do *not* emulate specific targets.

Experimental Biases

Targeted Attacks

We do *not* emulate specific targets.

DarkComet

DarkComet is a favorite of script kiddies.

Experimental Biases

Targeted Attacks

We do *not* emulate specific targets.

DarkComet

DarkComet is a favorite of script kiddies.

Infection Longevity

One hour time limit prevents return.

Experimental Biases

Targeted Attacks

We do *not* emulate specific targets.

DarkComet

DarkComet is a favorite of script kiddies.

Infection Longevity

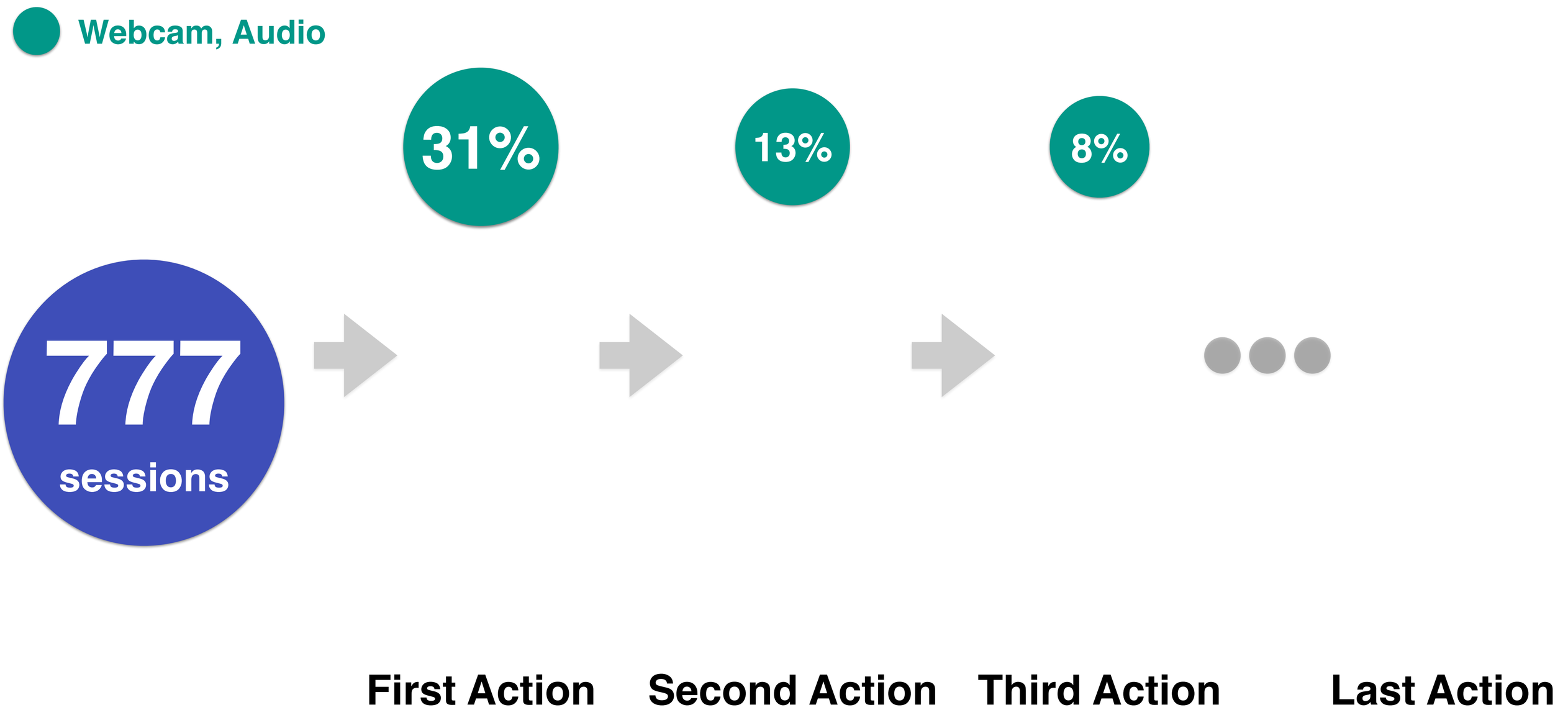
One hour time limit prevents return.

Honeypot Limitations

- No webcam or microphone feeds
- No responses to attacker-initiated chat, communication
- No keystrokes for keylogger
- Virtual machine indicators
- **Network containment policy**

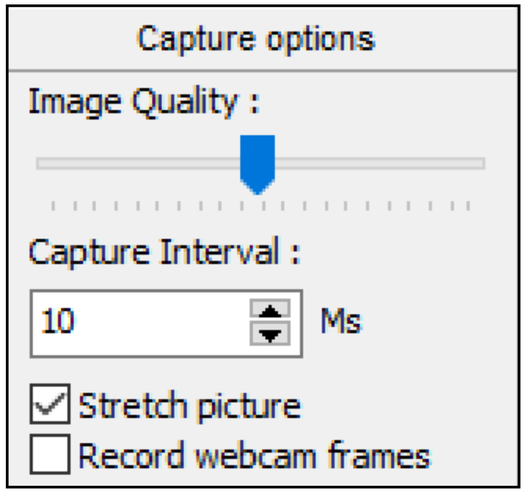
Common Patterns of Action

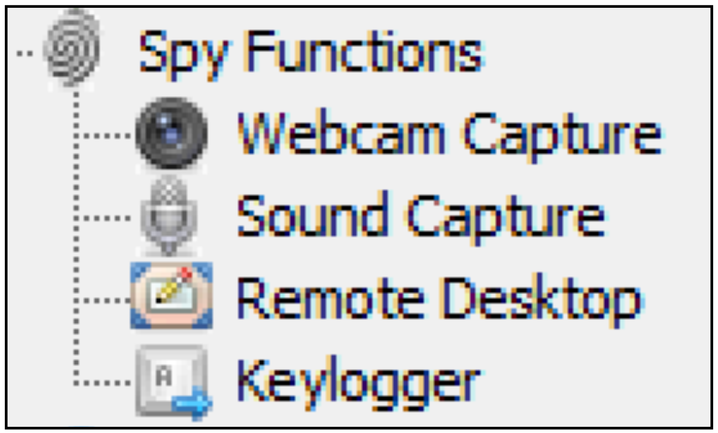
Common Patterns of Action



(Attempted) User Monitoring

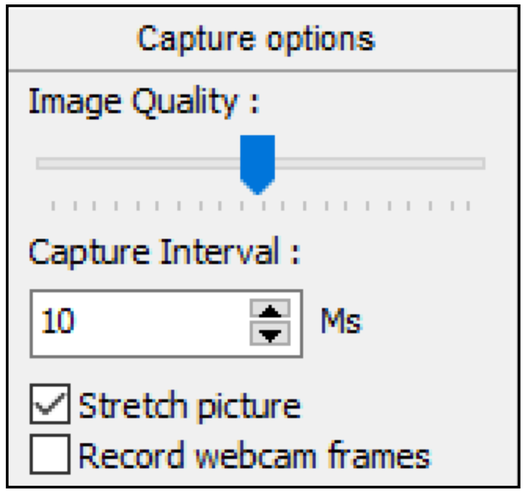
(Attempted) User Monitoring

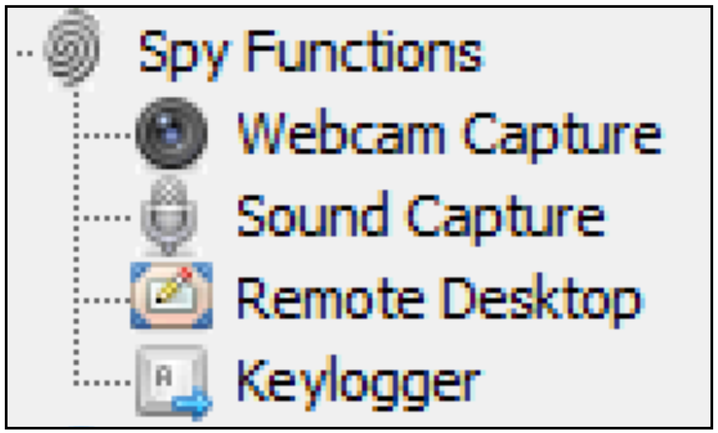


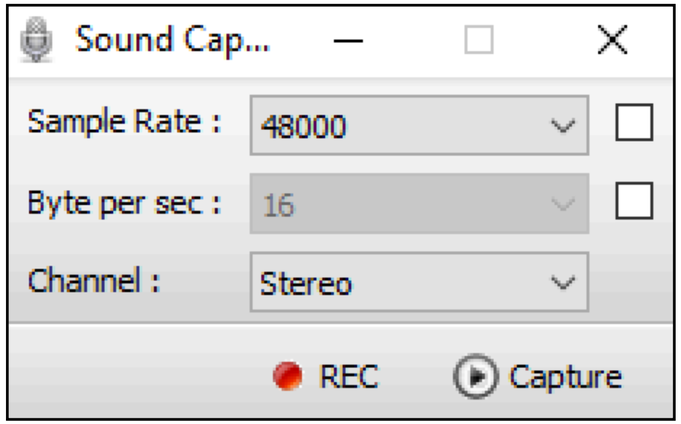


Webcam: **61%**

(Attempted) User Monitoring



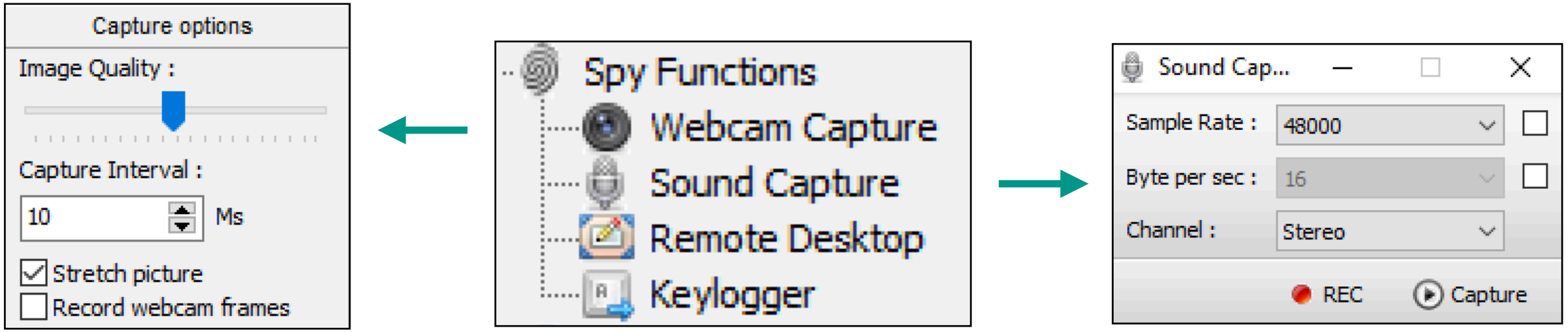




Webcam: **61%**

Microphone: **26%**

(Attempted) User Monitoring

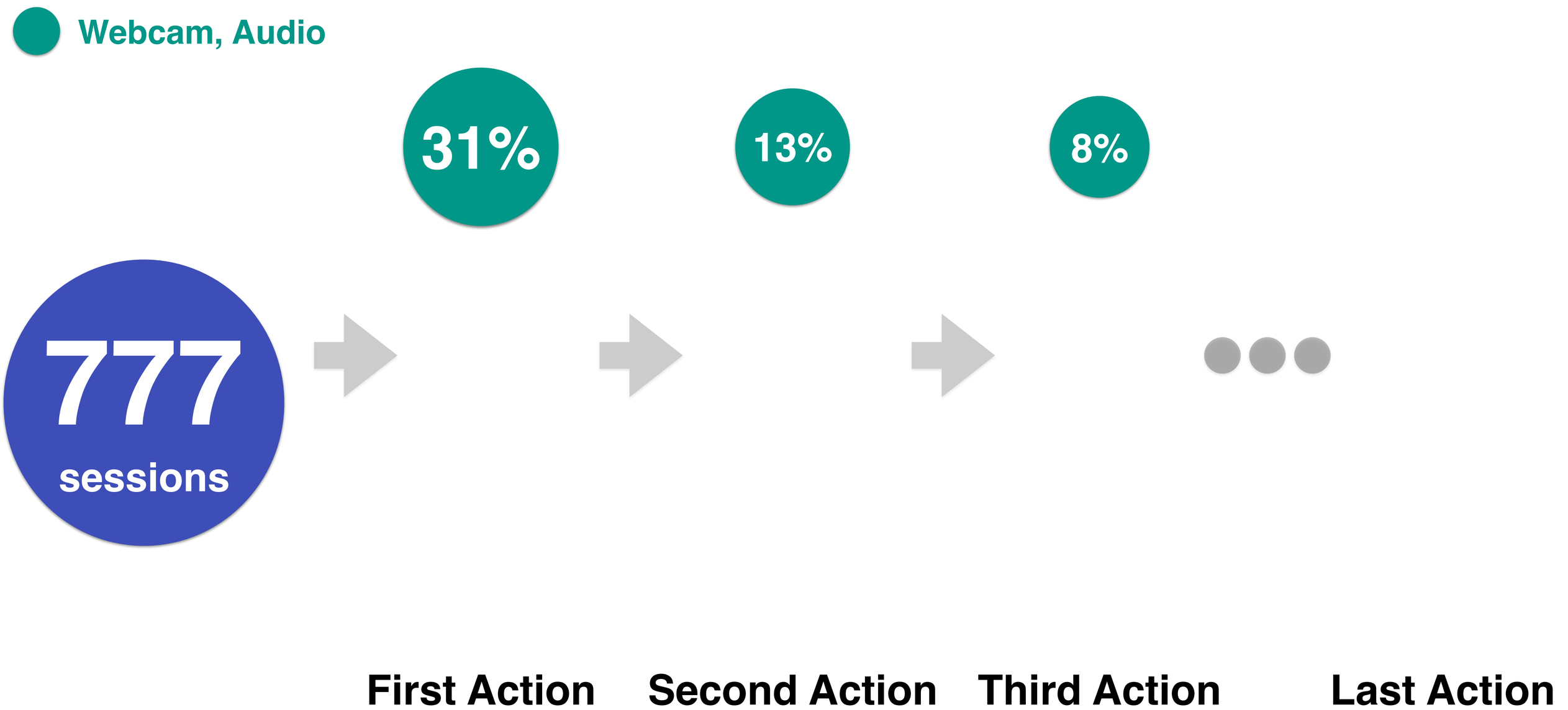


Webcam: **61%**

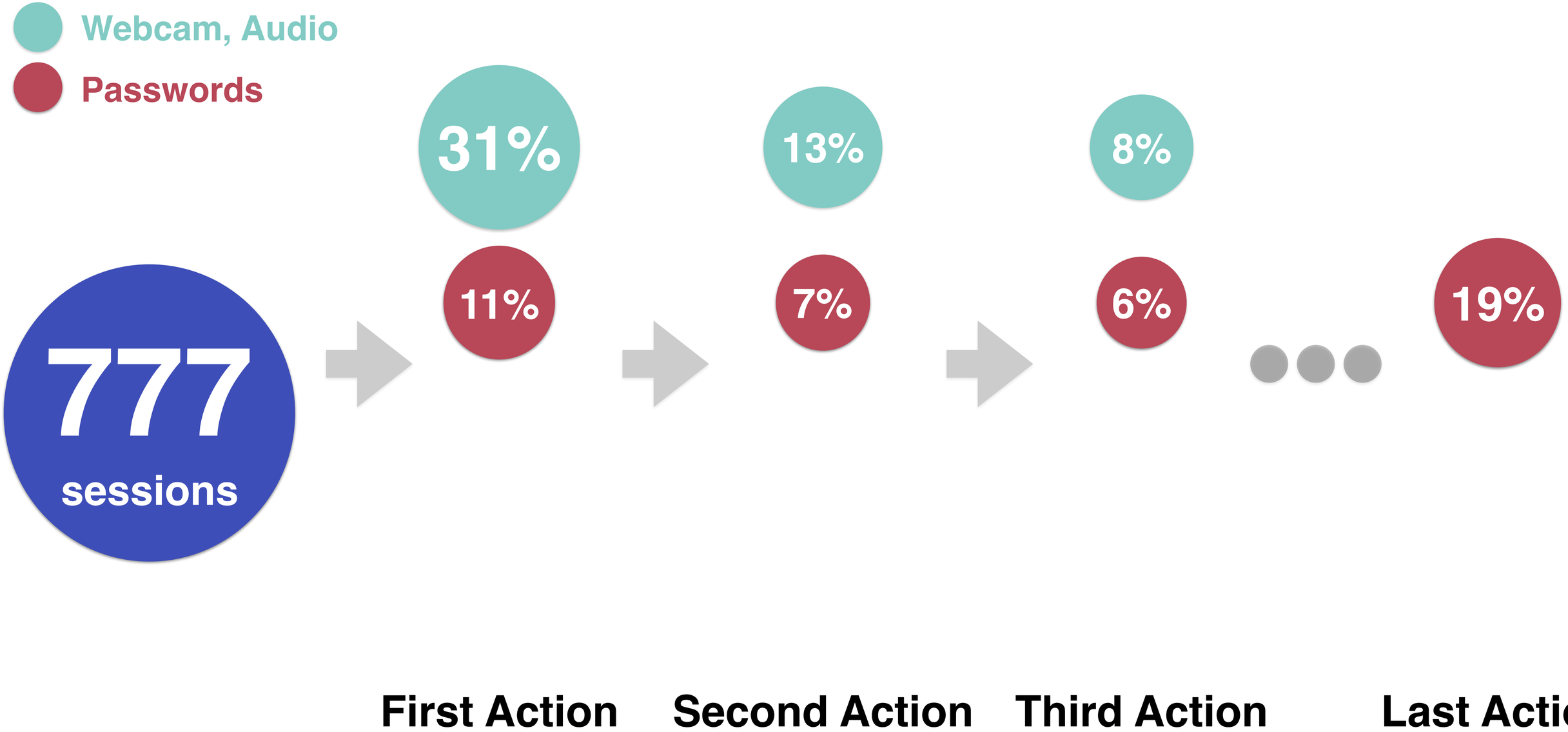
Microphone: **26%**

- Recall: We do **not** provide webcam / microphone feeds
- Motivation unknown!

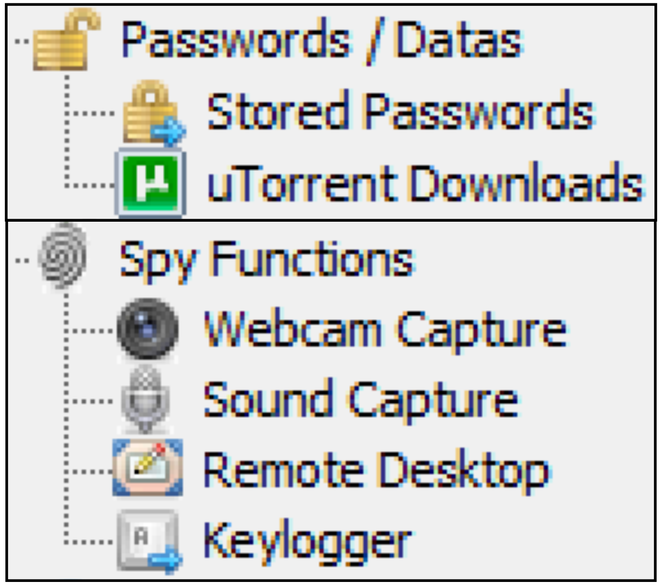
Common Patterns of Action



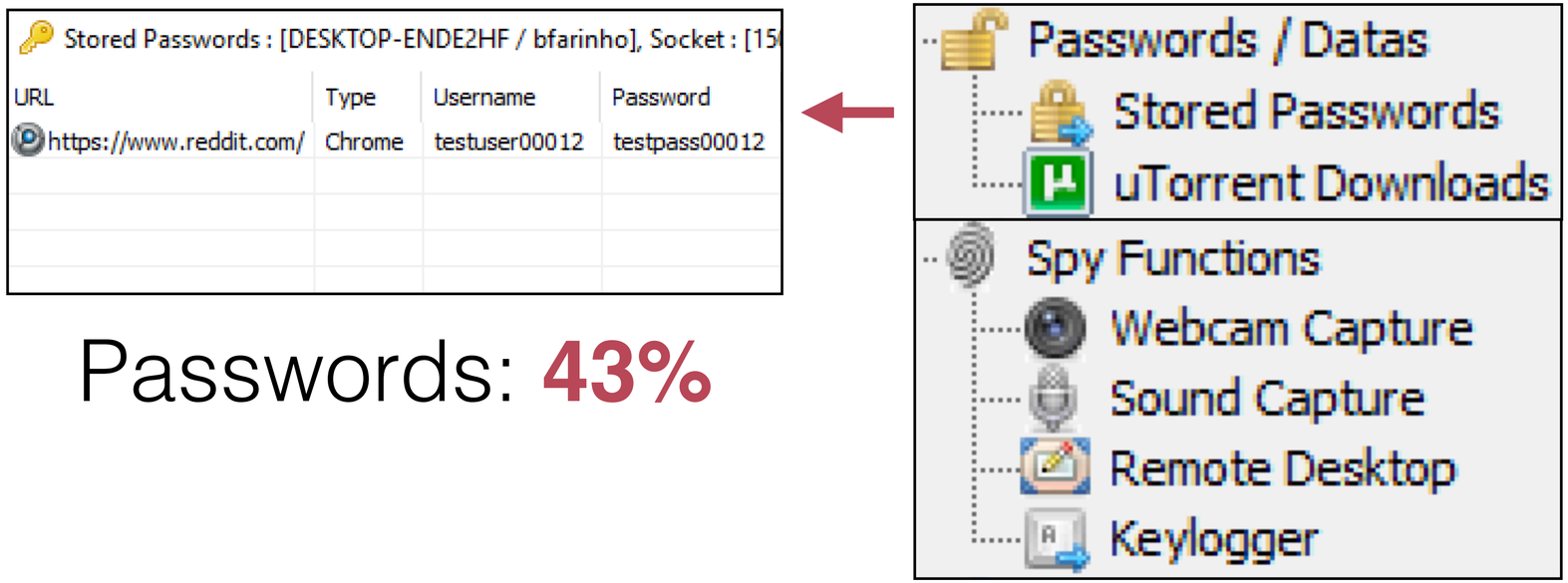
Common Patterns of Action



Credential Theft



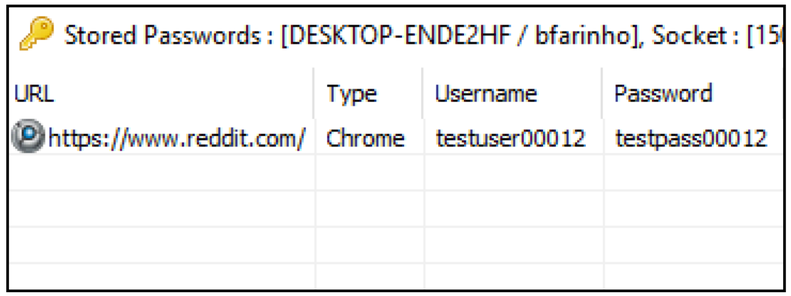
Credential Theft



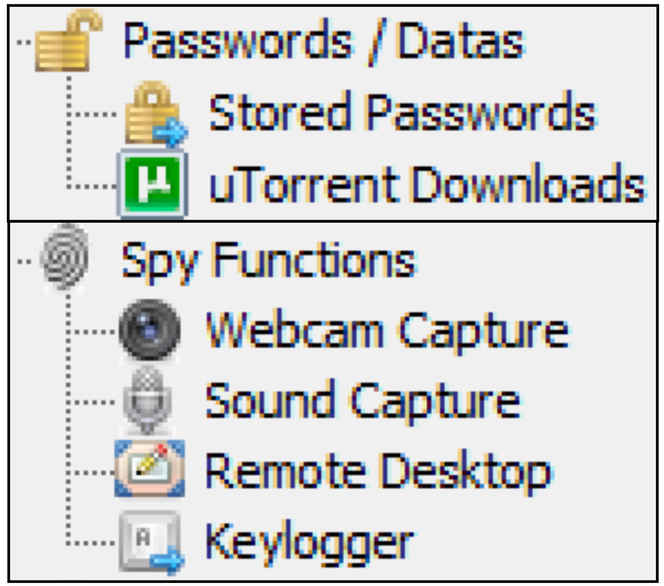
Passwords: **43%**

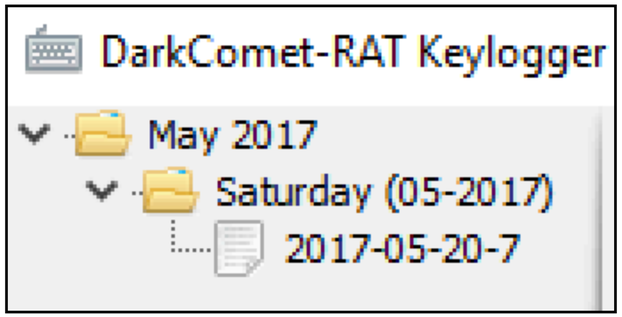
- Credentials seeded on honeypots were used **13** times outside study
- **Steam** (gaming platform) was probed often

Credential Theft



Passwords: **43%**

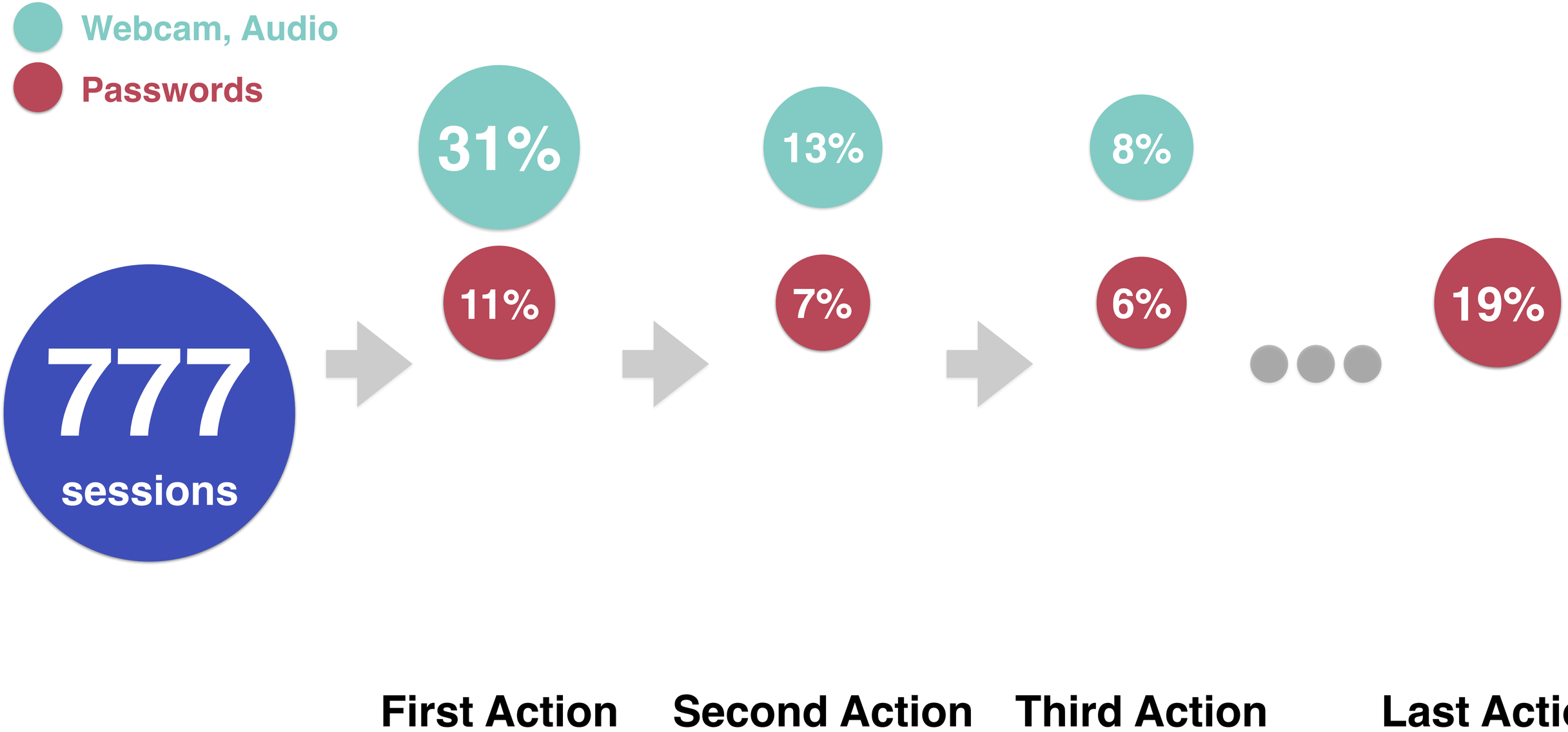




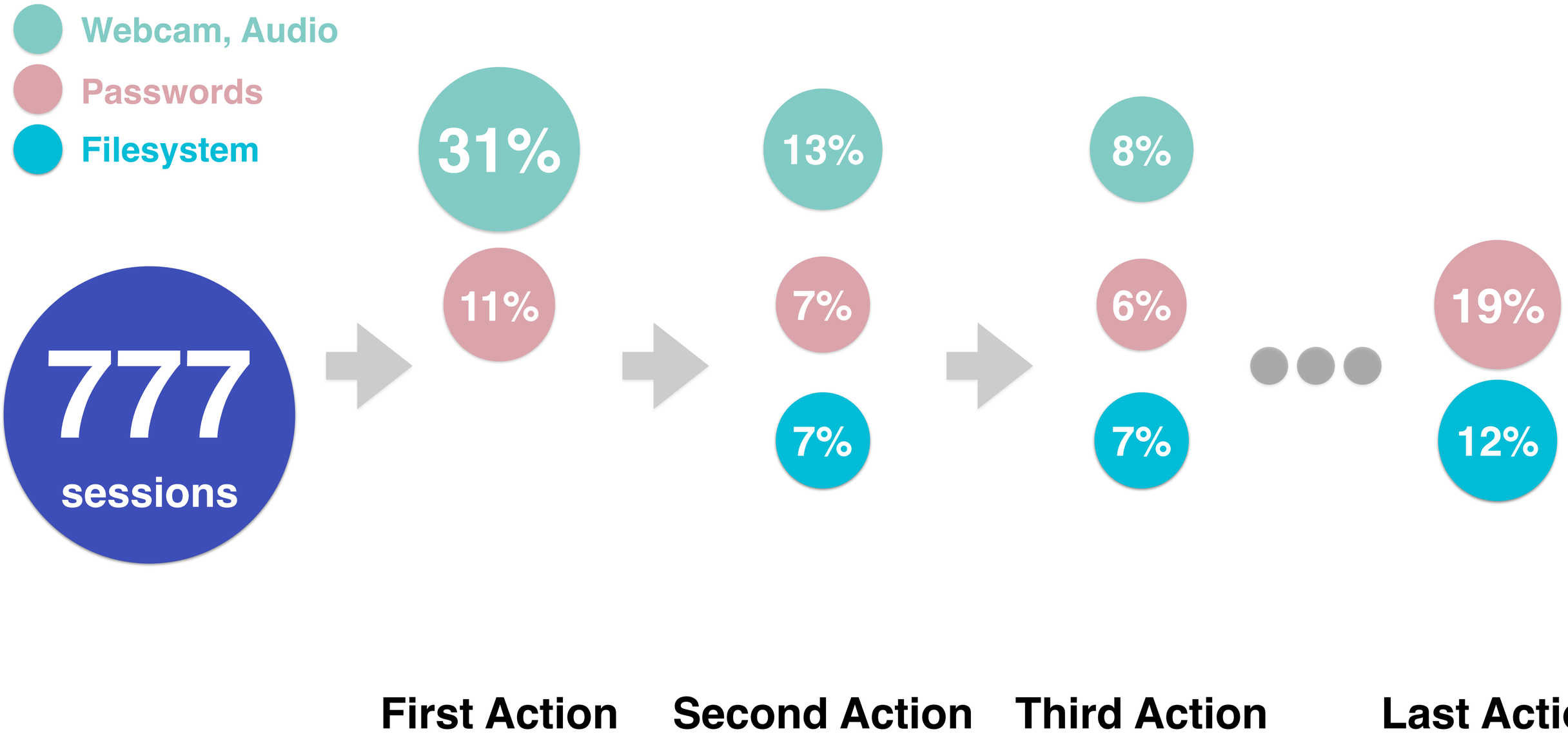
Keylogger: **31%**

- Credentials seeded on honeypots were used **13** times outside study
- **Steam** (gaming platform) was probed often
- For one-click actions, these numbers are low… Recreational users?

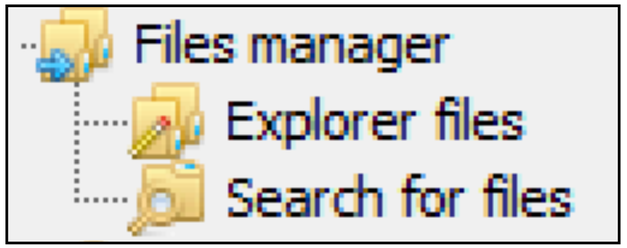
Common Patterns of Action



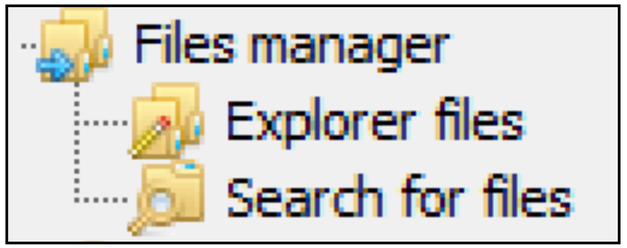
Common Patterns of Action



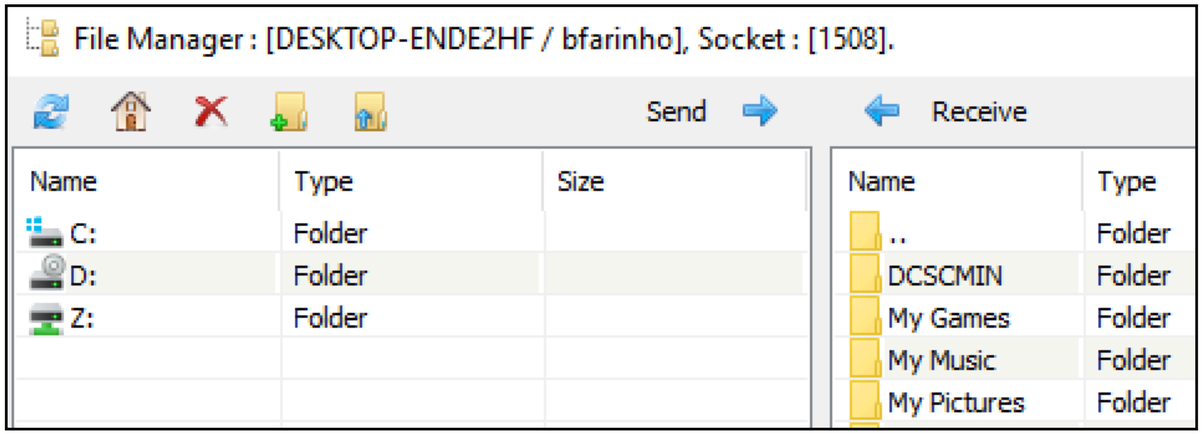
Filesystem Access



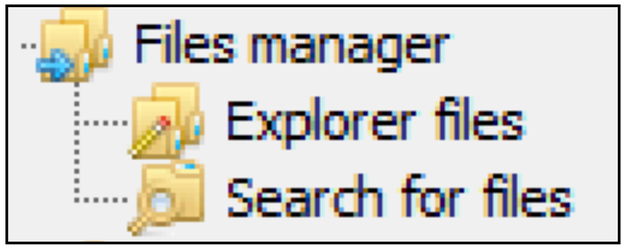
Filesystem Access



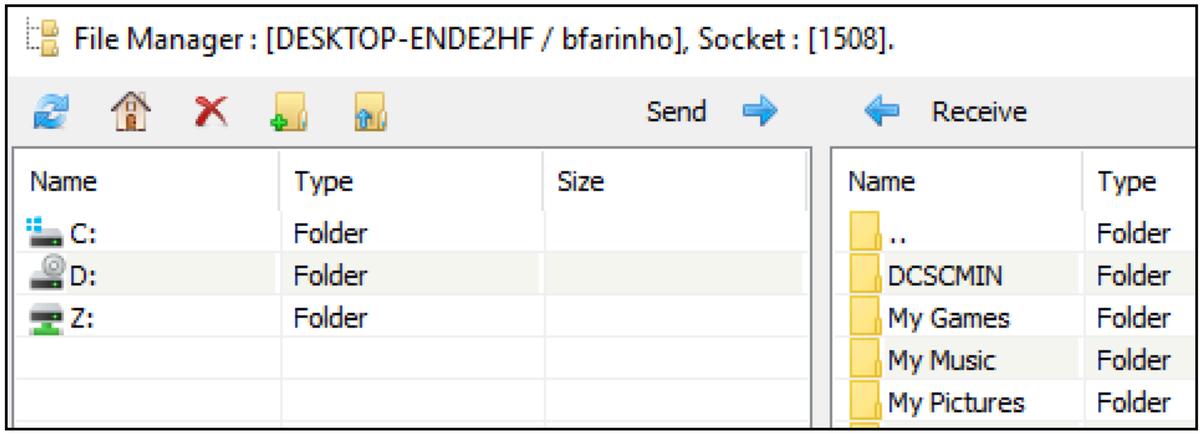
Filesystem Exploration: **40%**



Filesystem Access



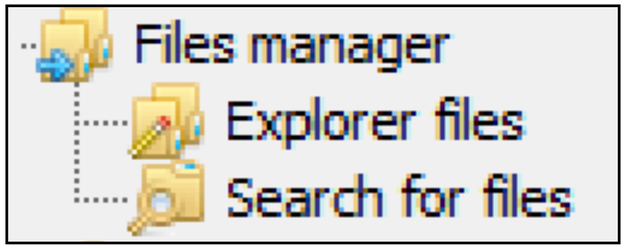
Filesystem Exploration: **40%**



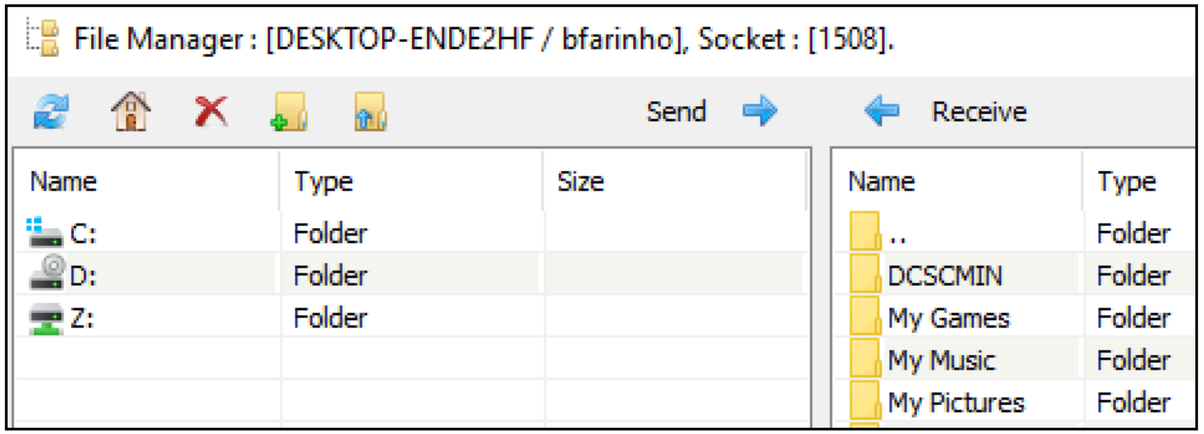
Upload: **18%**

- **4%** of attackers uploaded hacking tools
- **34** unique executables uploaded, **19** new to VirusTotal

Filesystem Access



Filesystem Exploration: **40%**

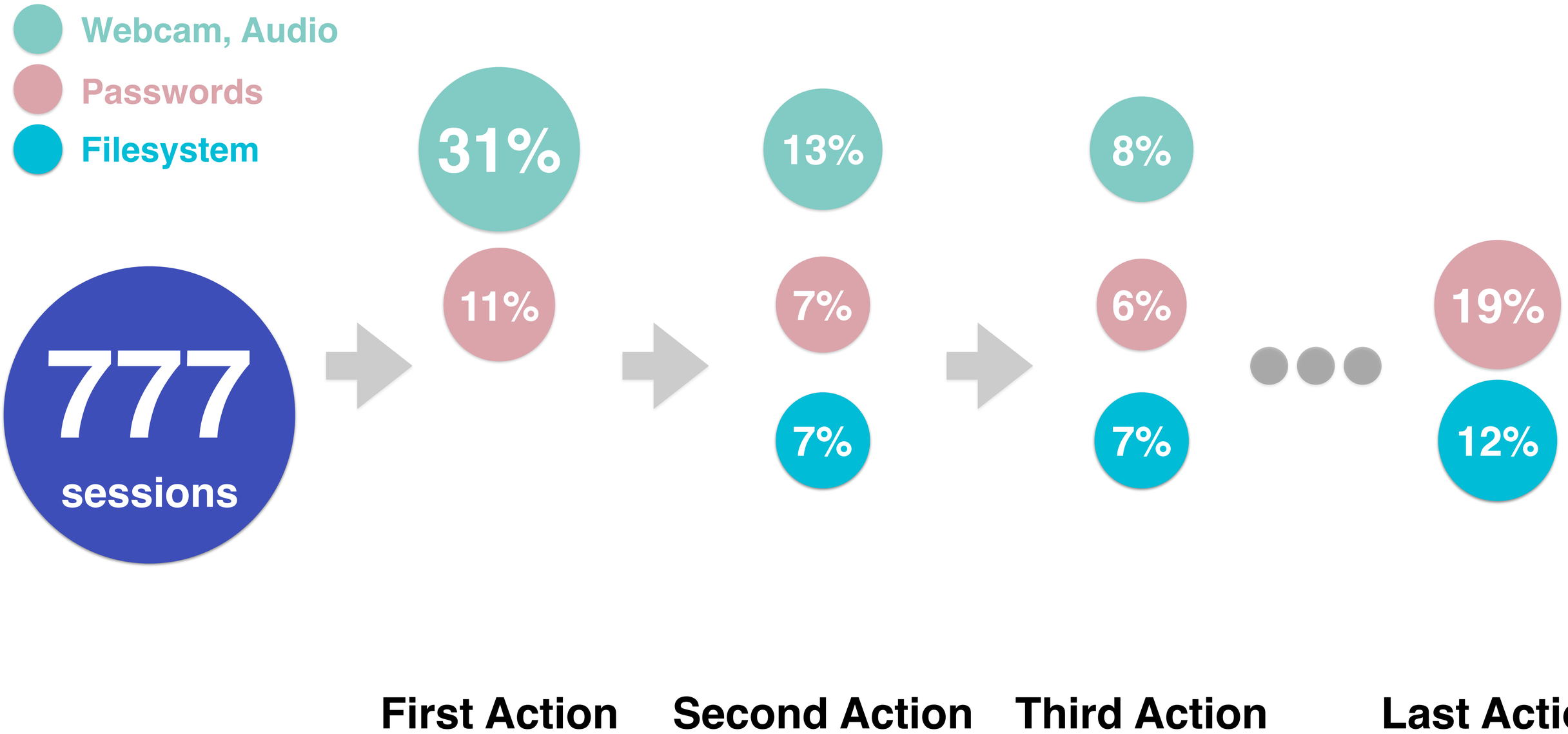


Upload: **18%**

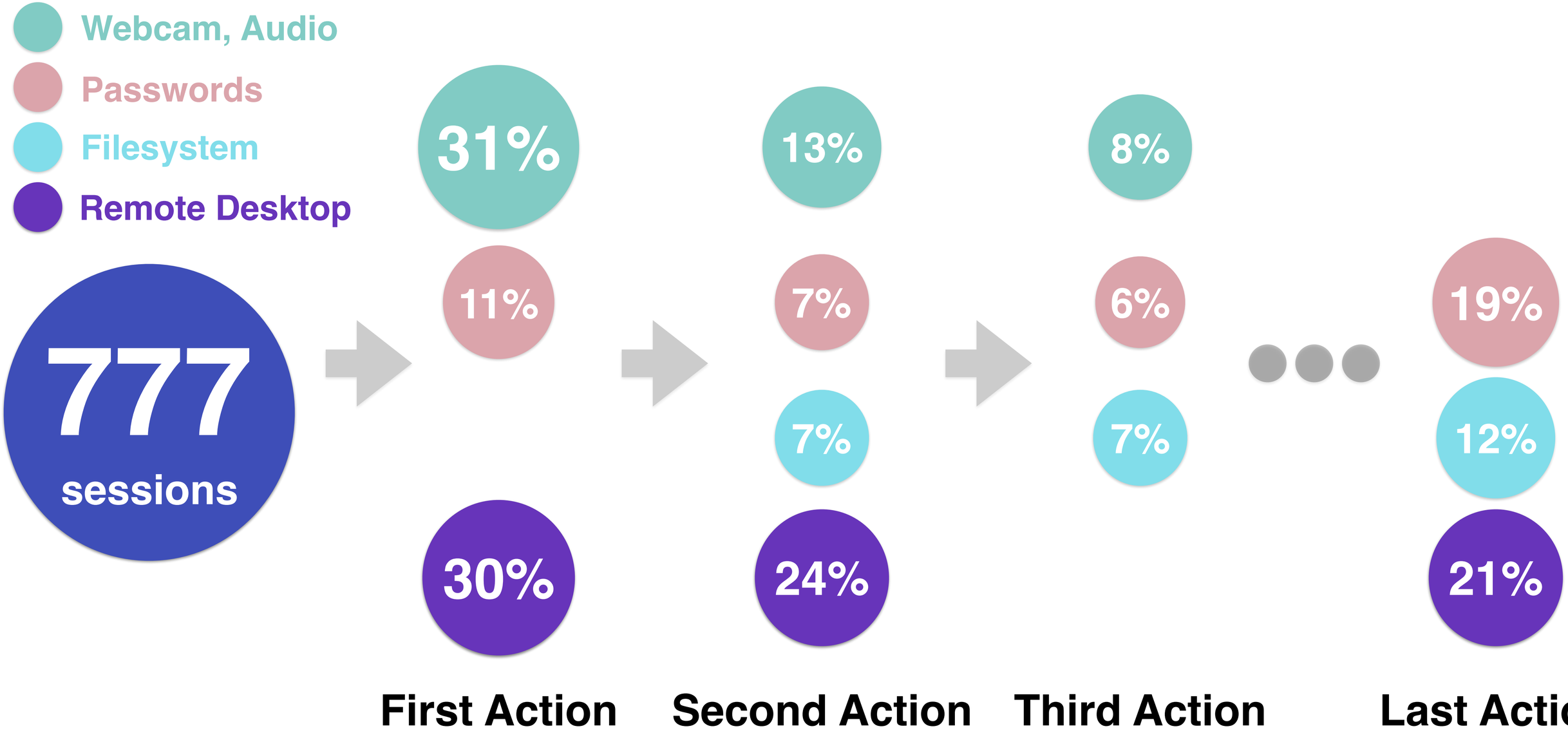
Download: **8%**

- **4%** of attackers uploaded hacking tools
- **34** unique executables uploaded, **19** new to VirusTotal
- Bitcoin wallets, Steam configs downloaded often

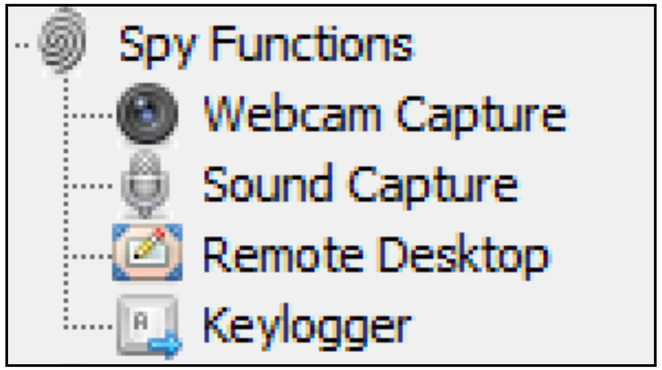
Common Patterns of Action



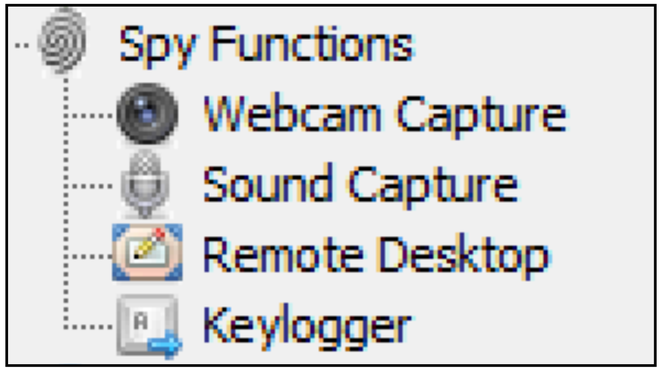
Common Patterns of Action



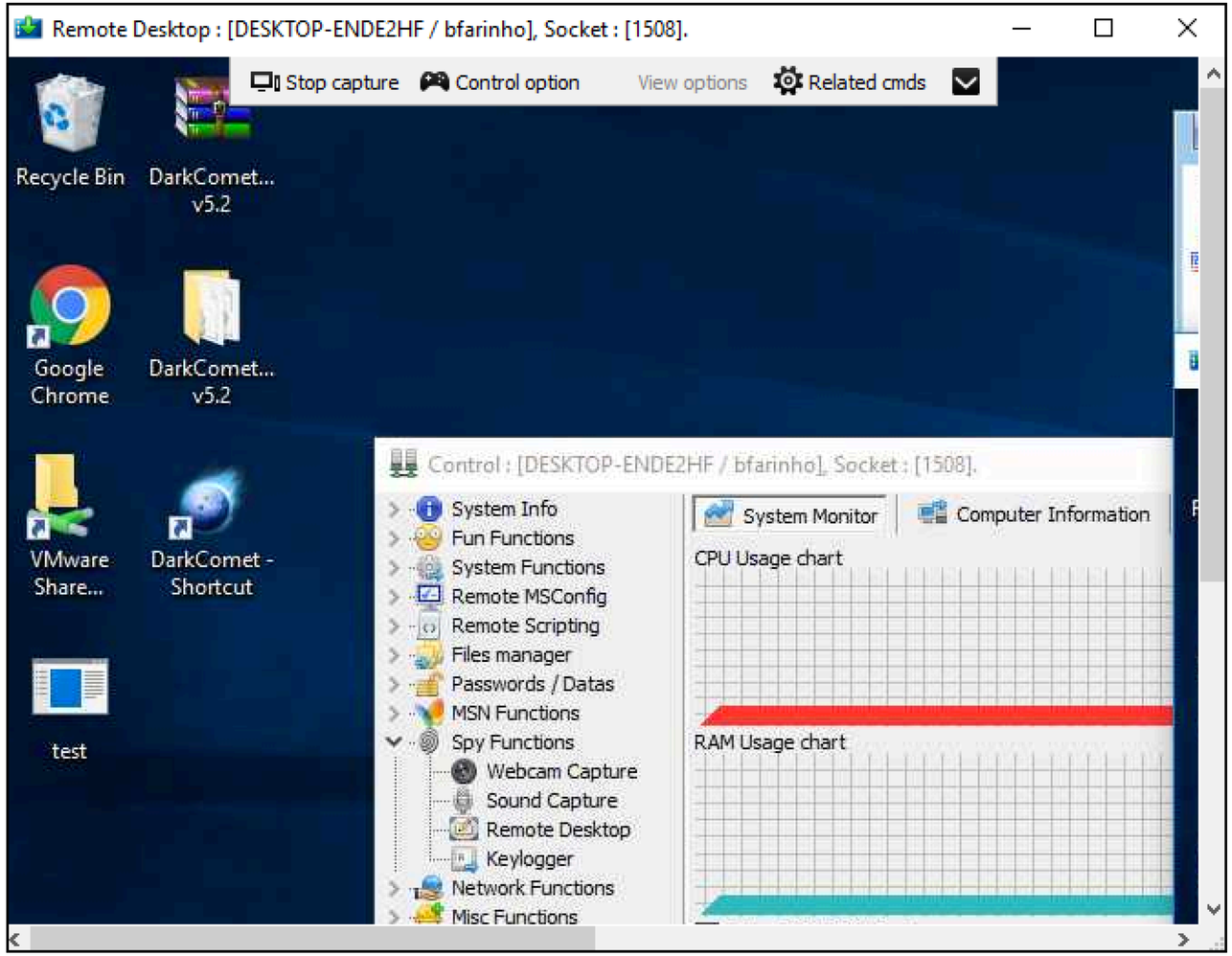
Remote Desktop



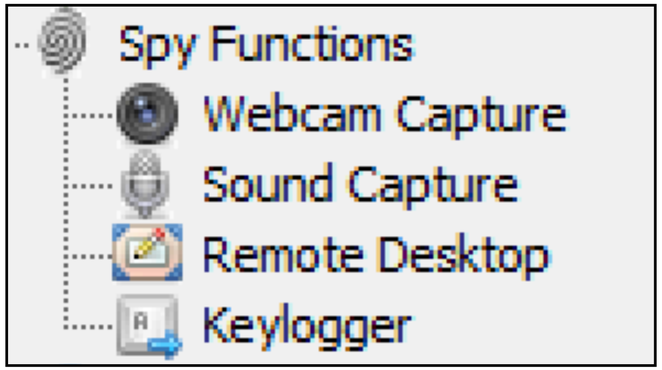
Remote Desktop

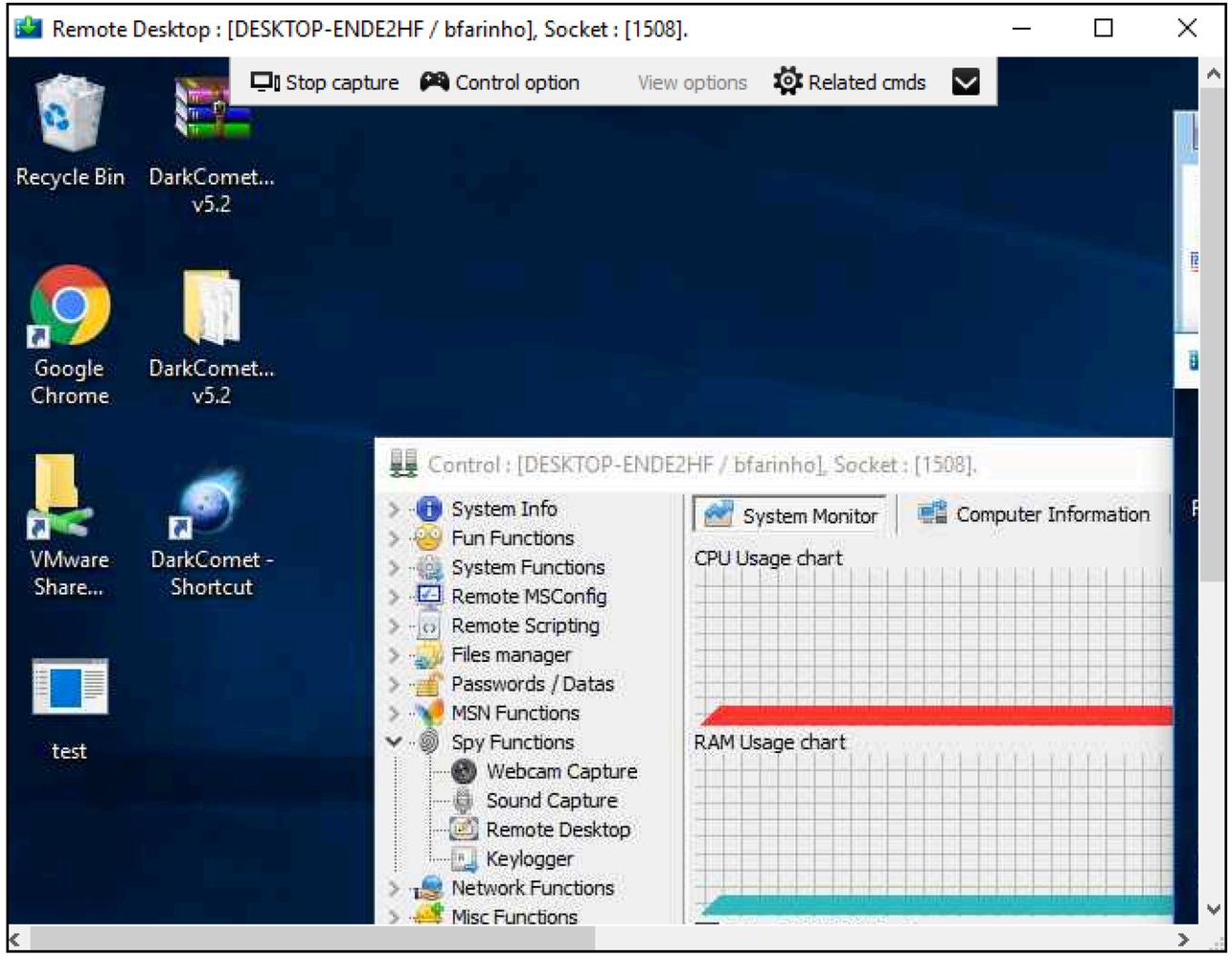


Remote Desktop: **83%** !



Remote Desktop



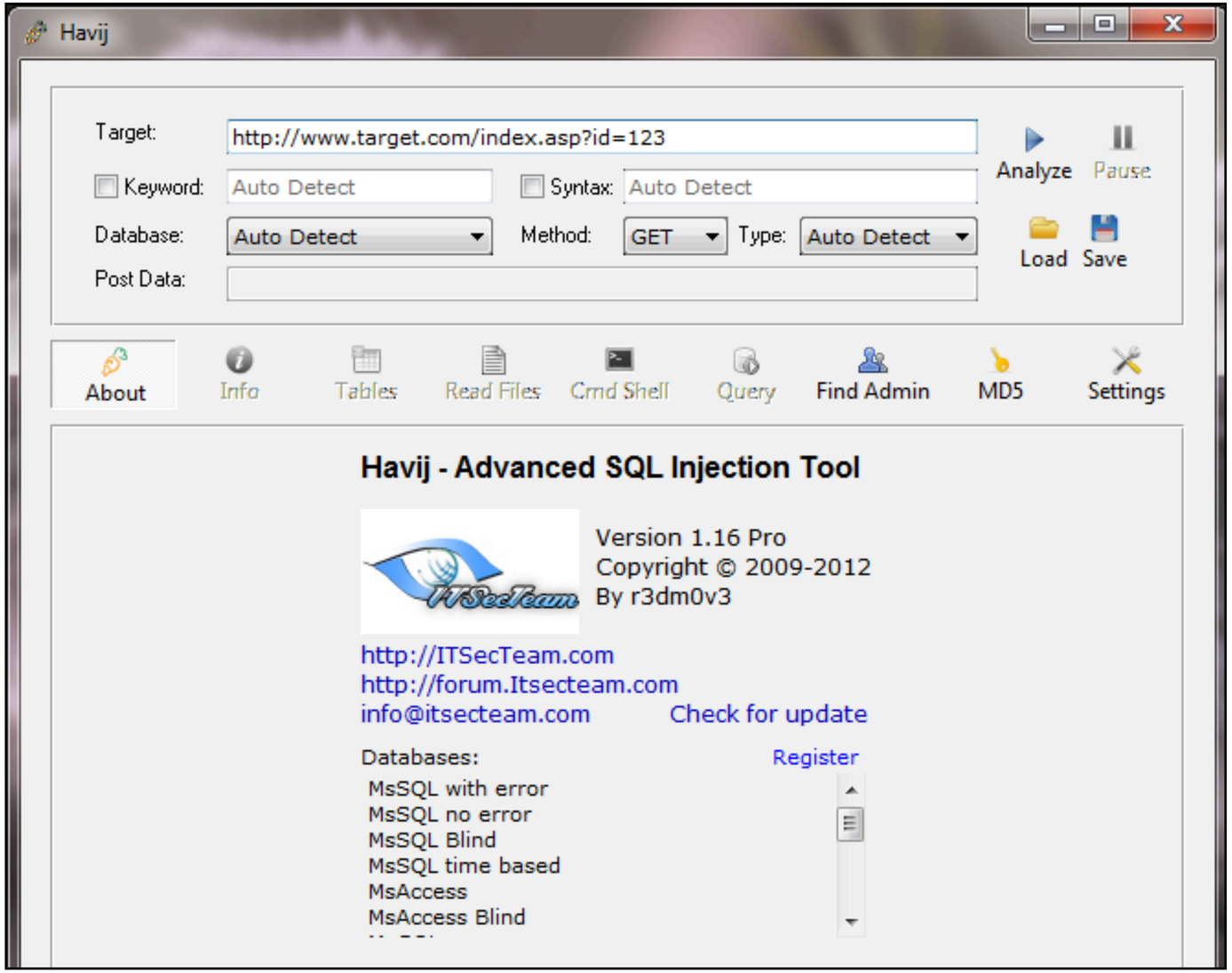


Remote Desktop: **83%** !

Active RD: **56%**

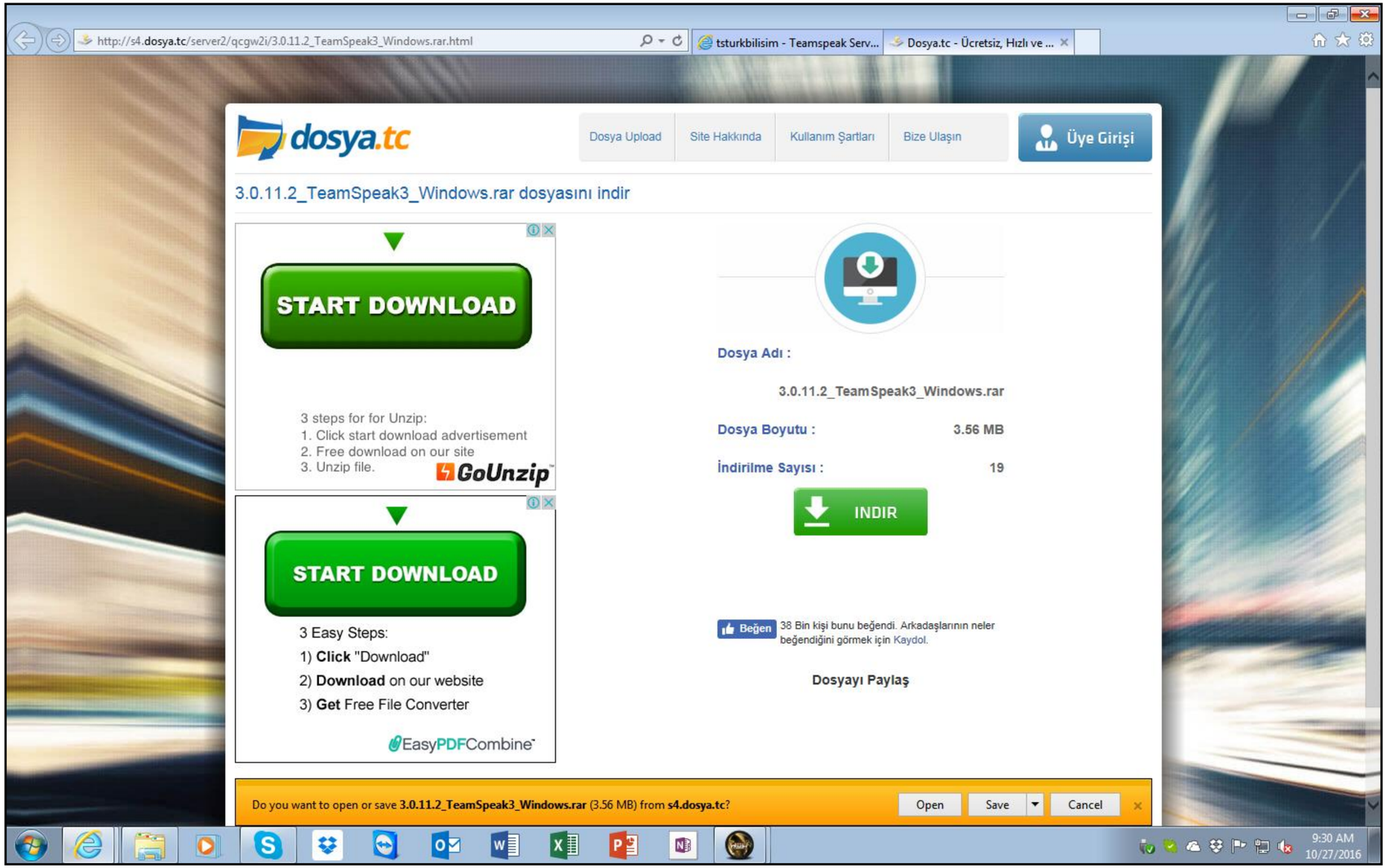
- GUI-based hacking tools
- Applications (Steam, browsers)

Remote Desktop



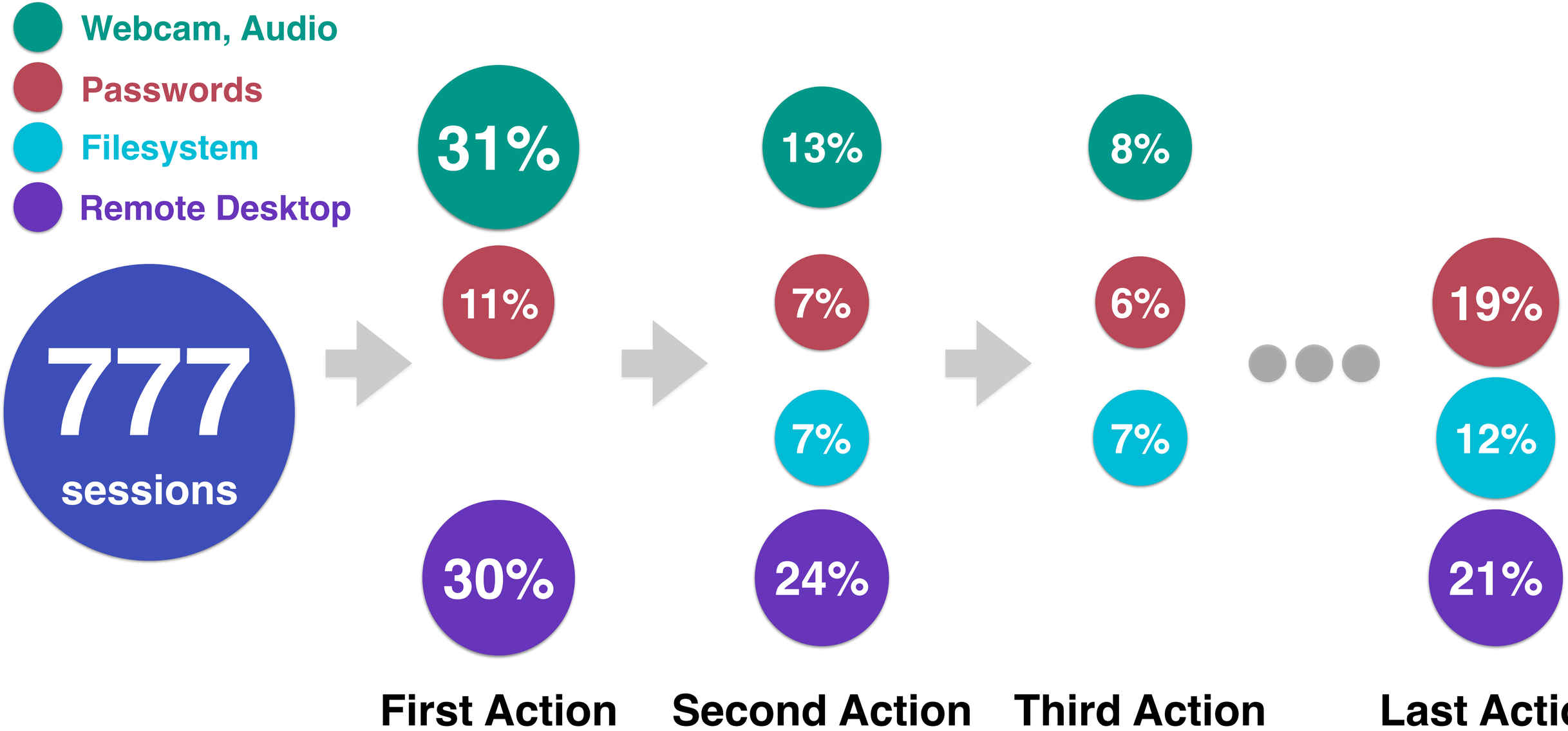
Havij SQL Injector

Remote Desktop

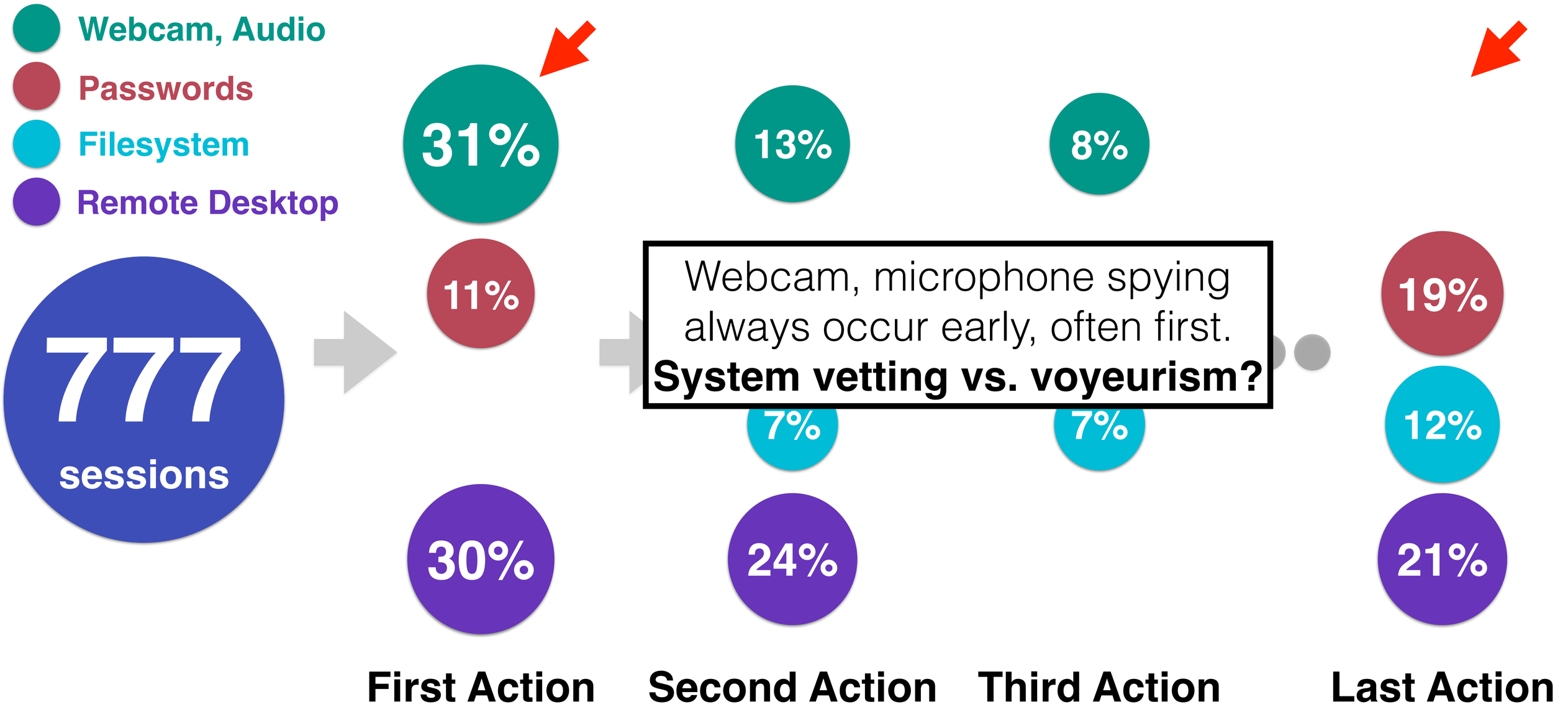


TeamSpeak 3 (gaming server)

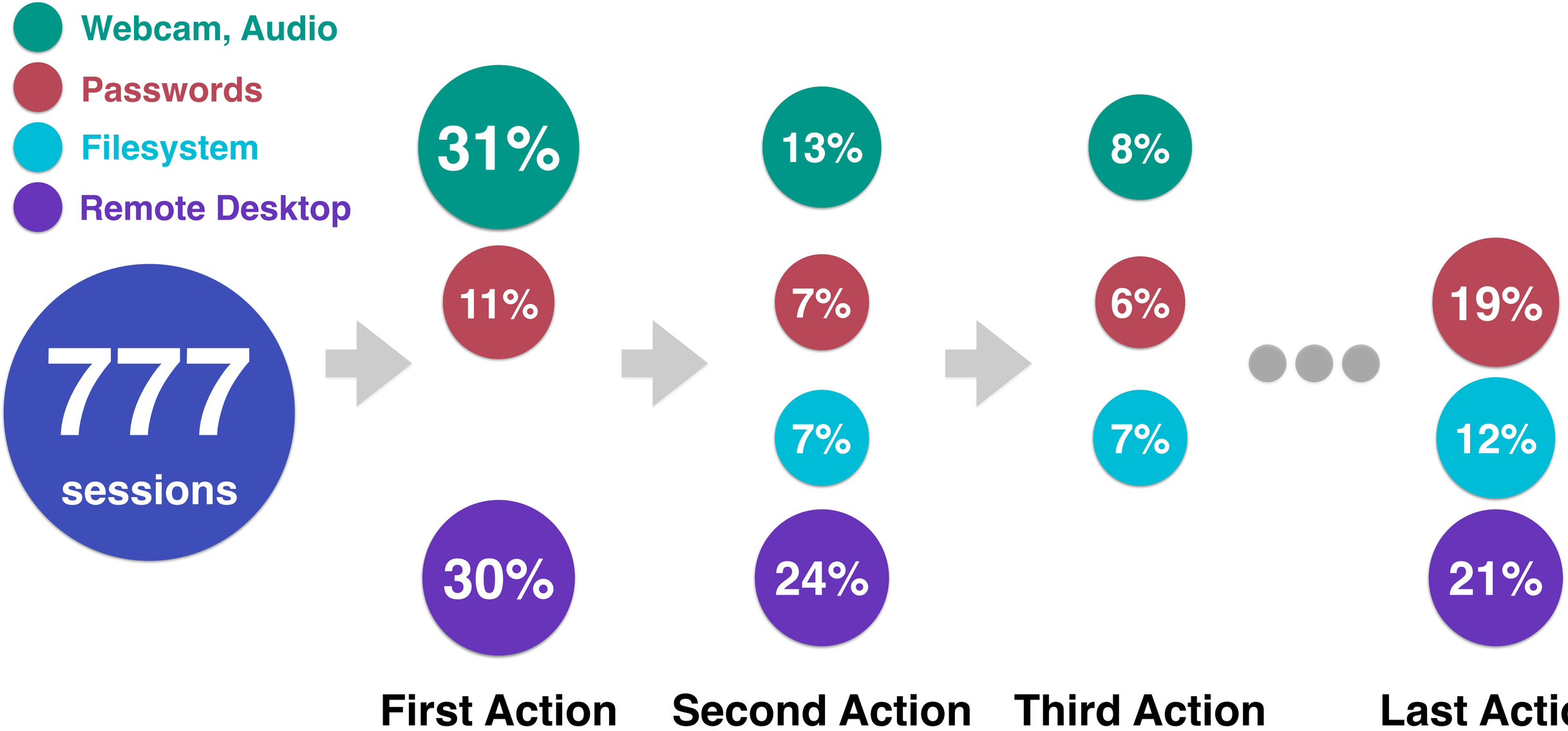
Common Patterns of Action



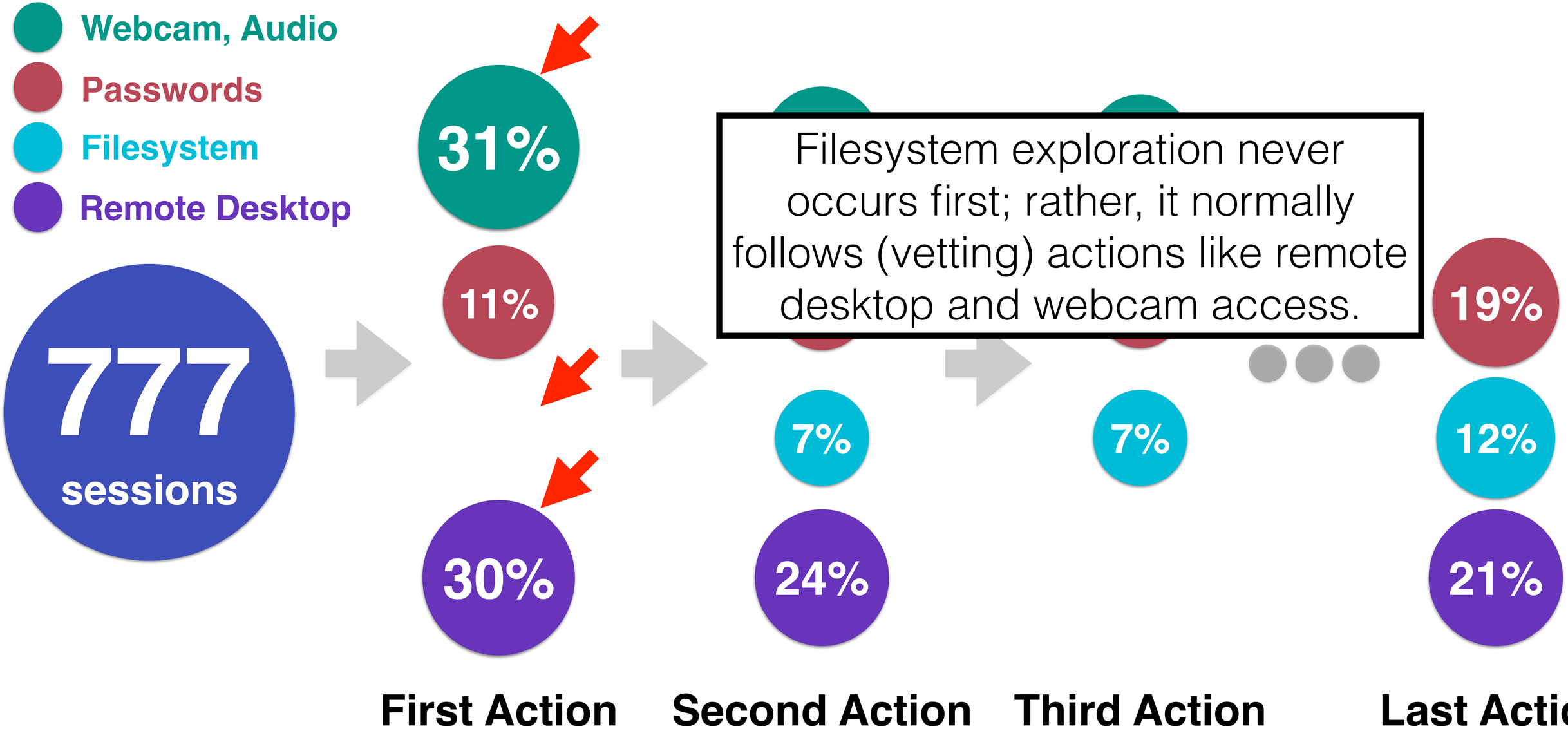
Common Patterns of Action



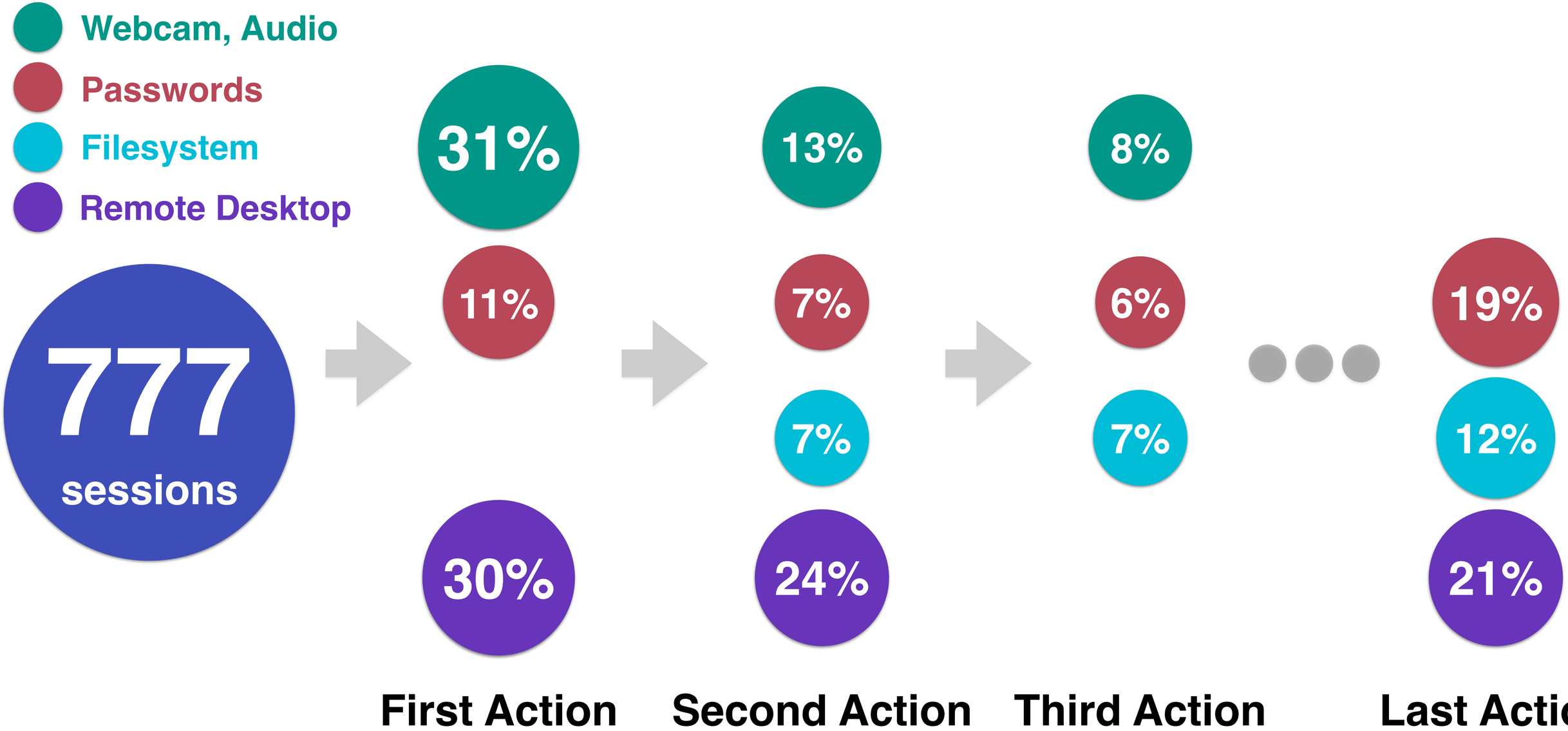
Common Patterns of Action



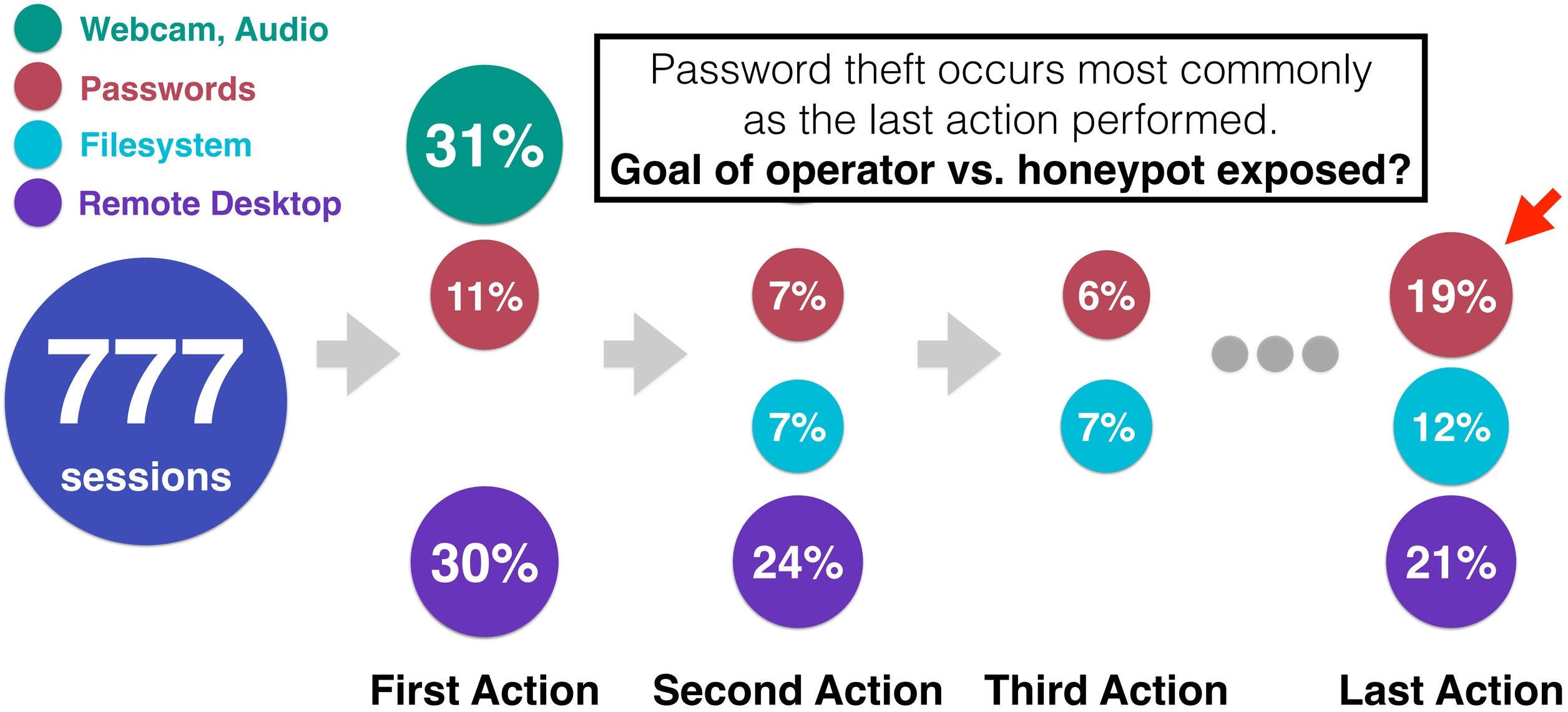
Common Patterns of Action



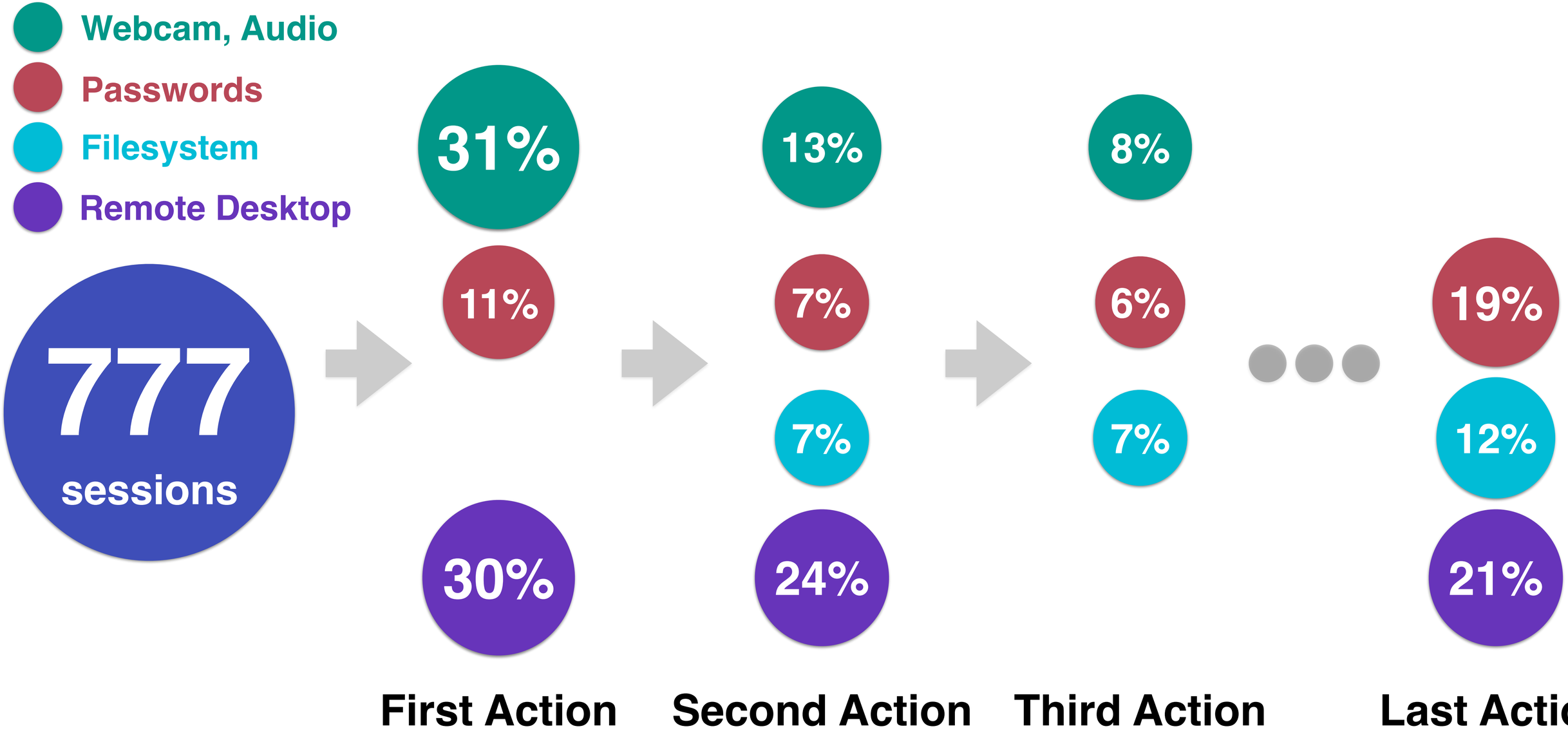
Common Patterns of Action



Common Patterns of Action

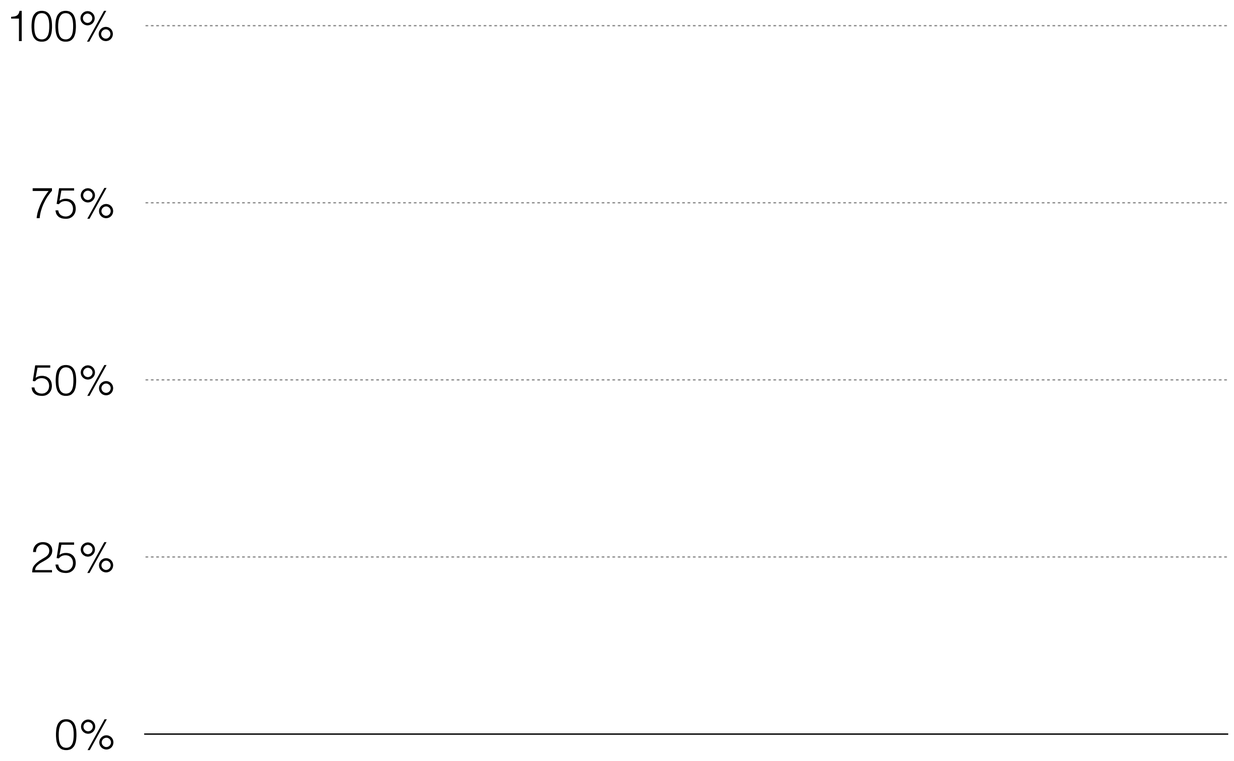


Common Patterns of Action



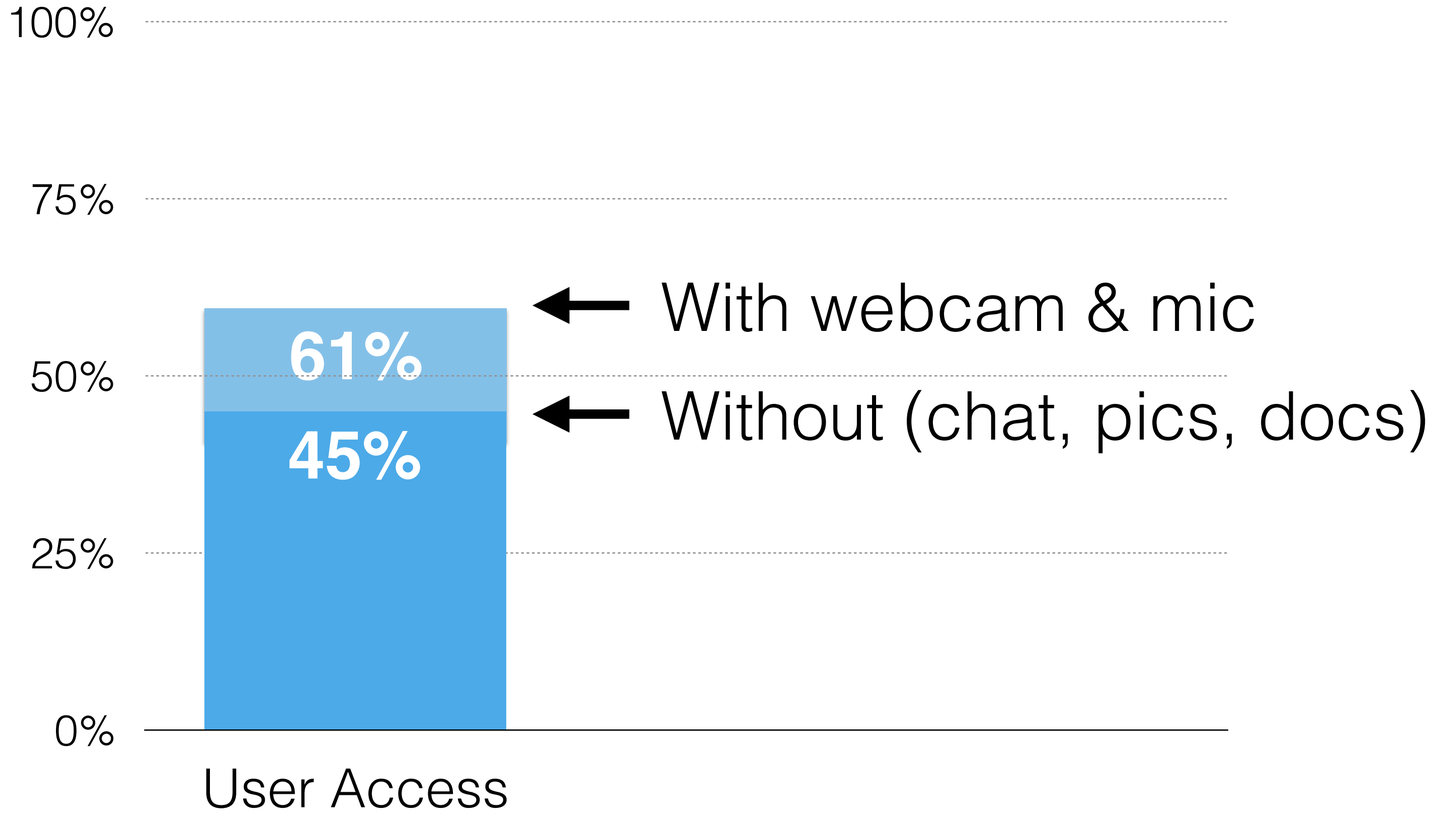
Overall Trends in Dataset

What **resource(s)** are RAT operators after?



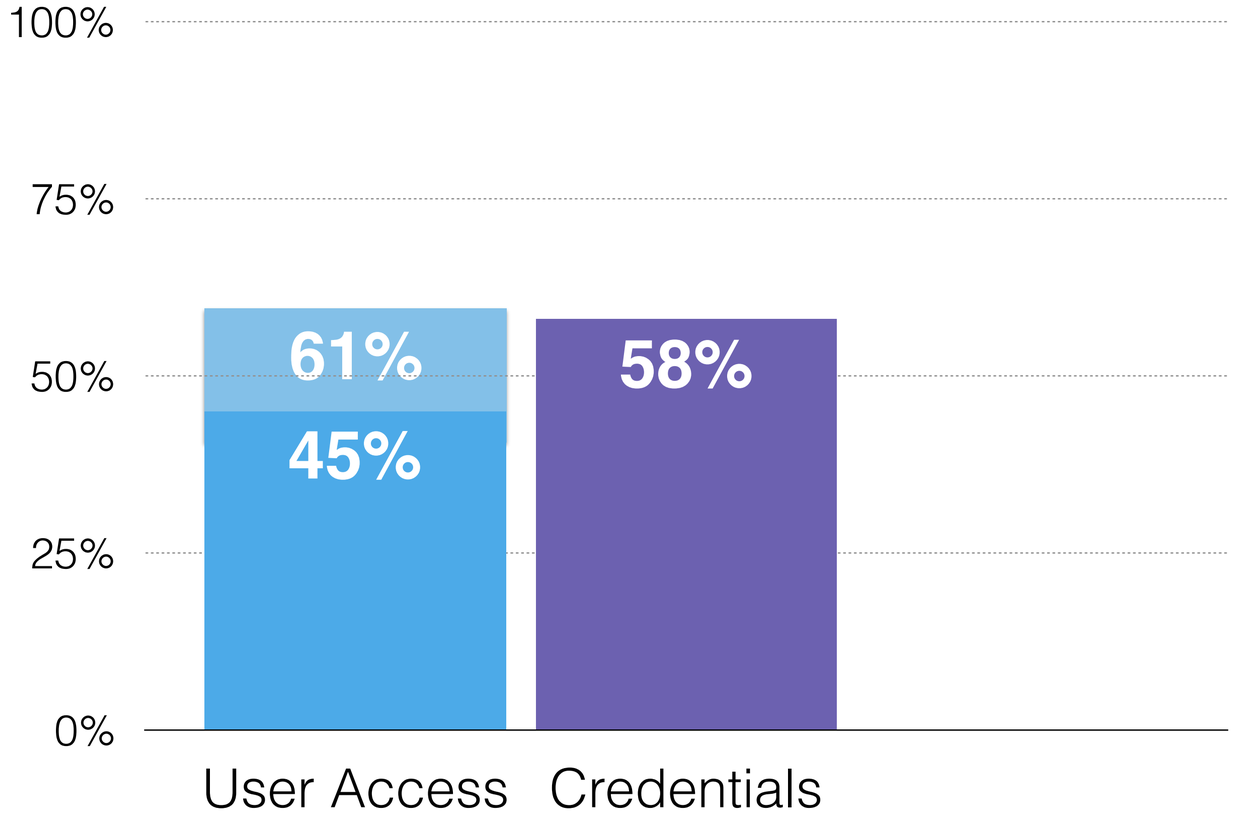
Overall Trends in Dataset

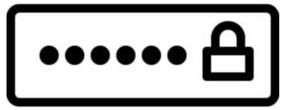
What **resource(s)** are RAT operators after?



Overall Trends in Dataset

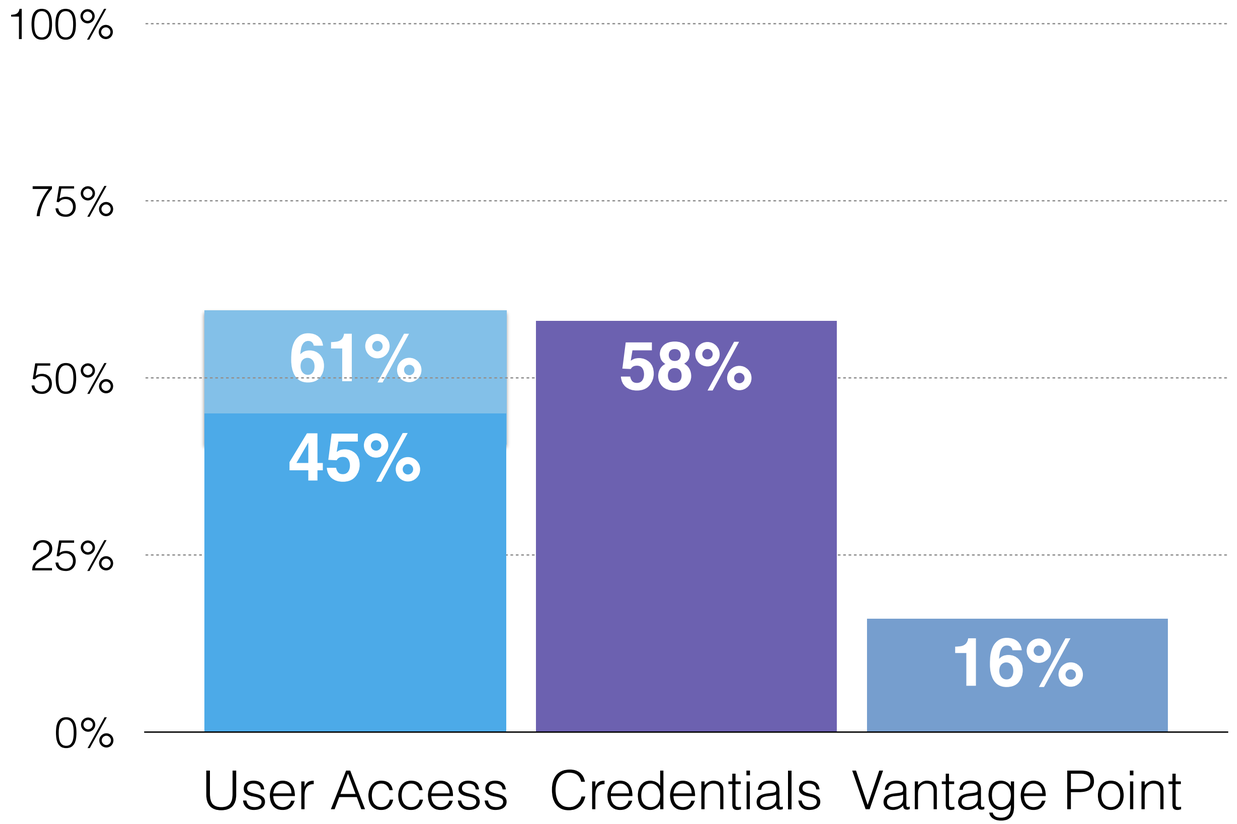
What **resource(s)** are RAT operators after?

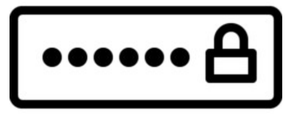


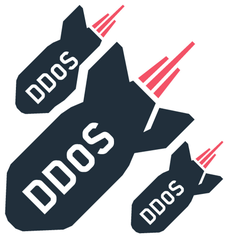


Overall Trends in Dataset

What **resource(s)** are RAT operators after?



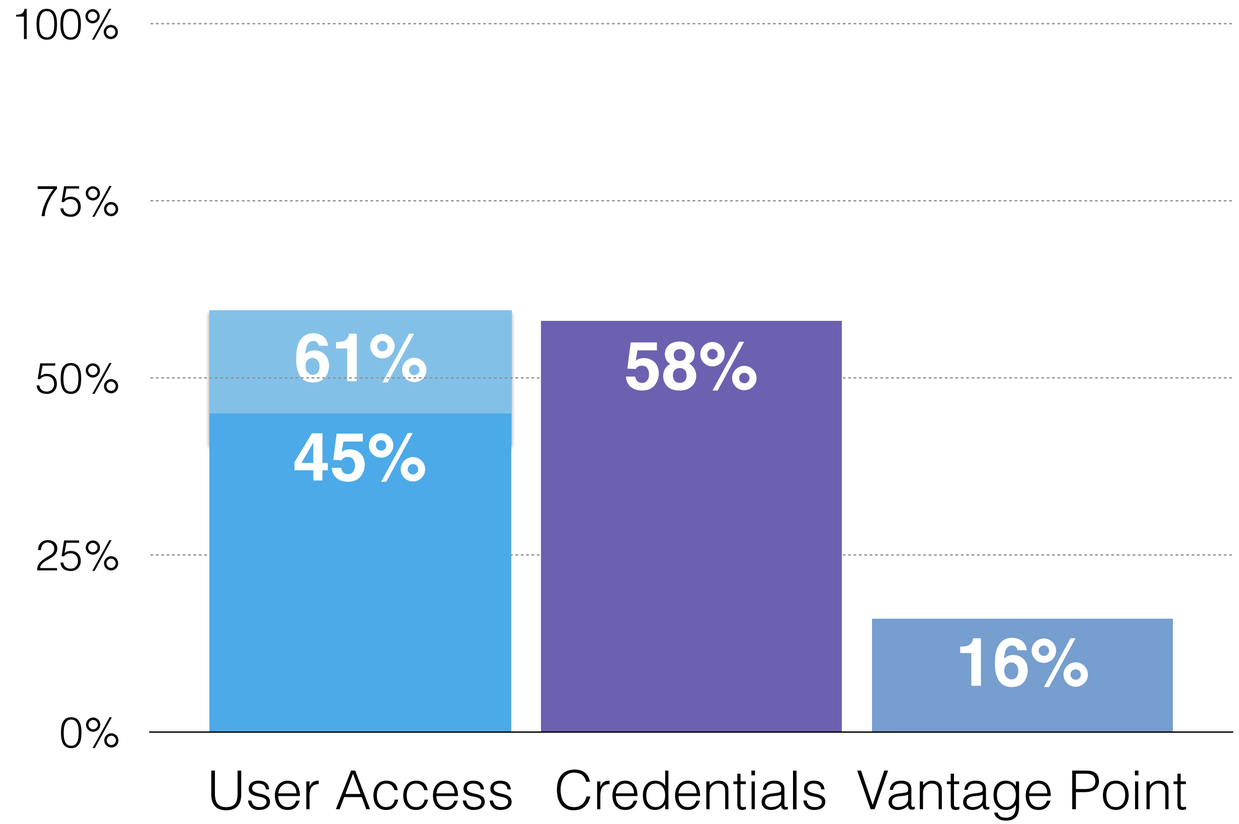


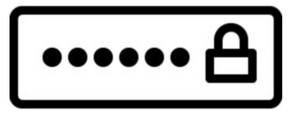


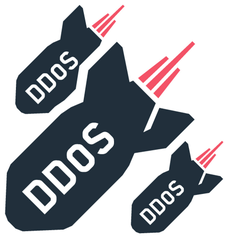
Overall Trends in Dataset

What **resource(s)** are RAT operators after?

- RATs are for user access



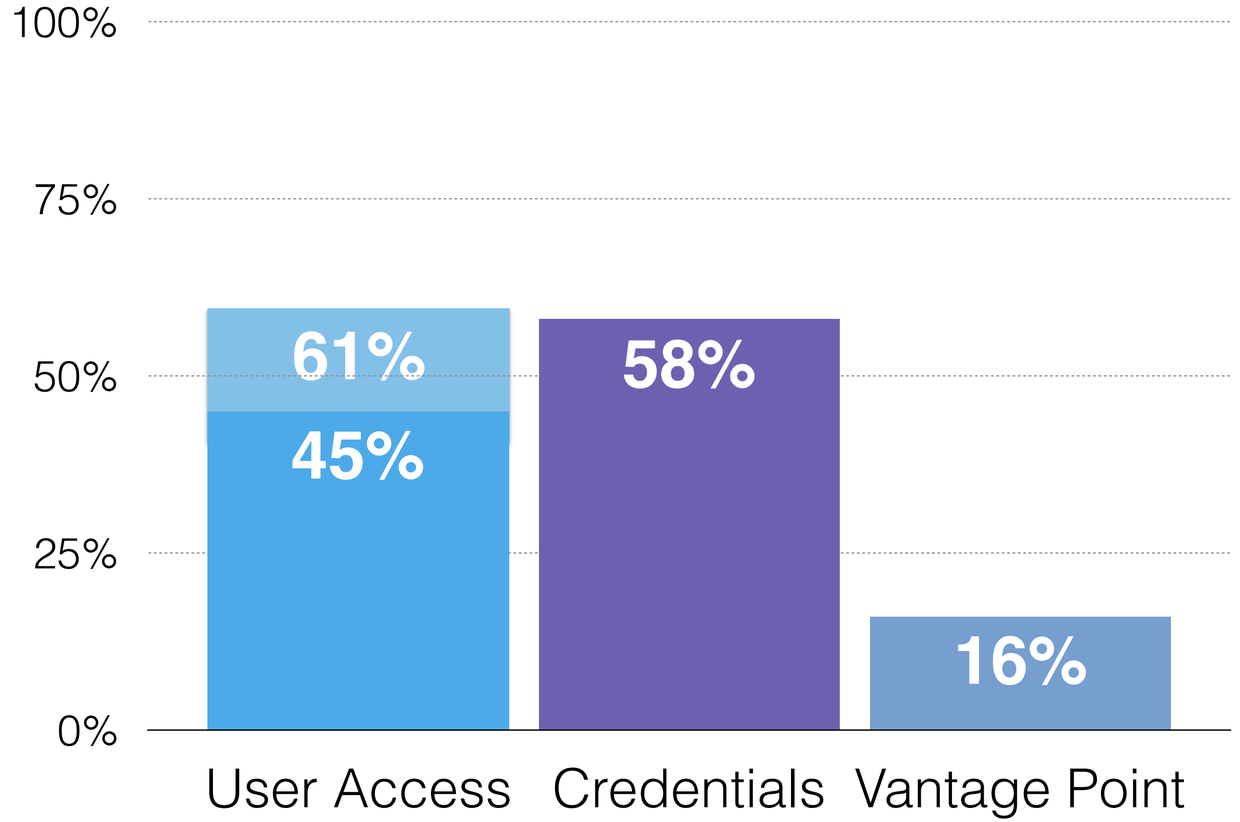


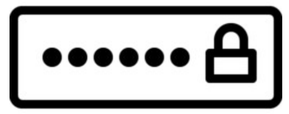


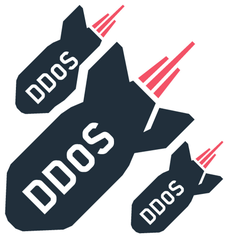
Overall Trends in Dataset

What **resource(s)** are RAT operators after?

- RATs are for user access
- RATs are easy, available



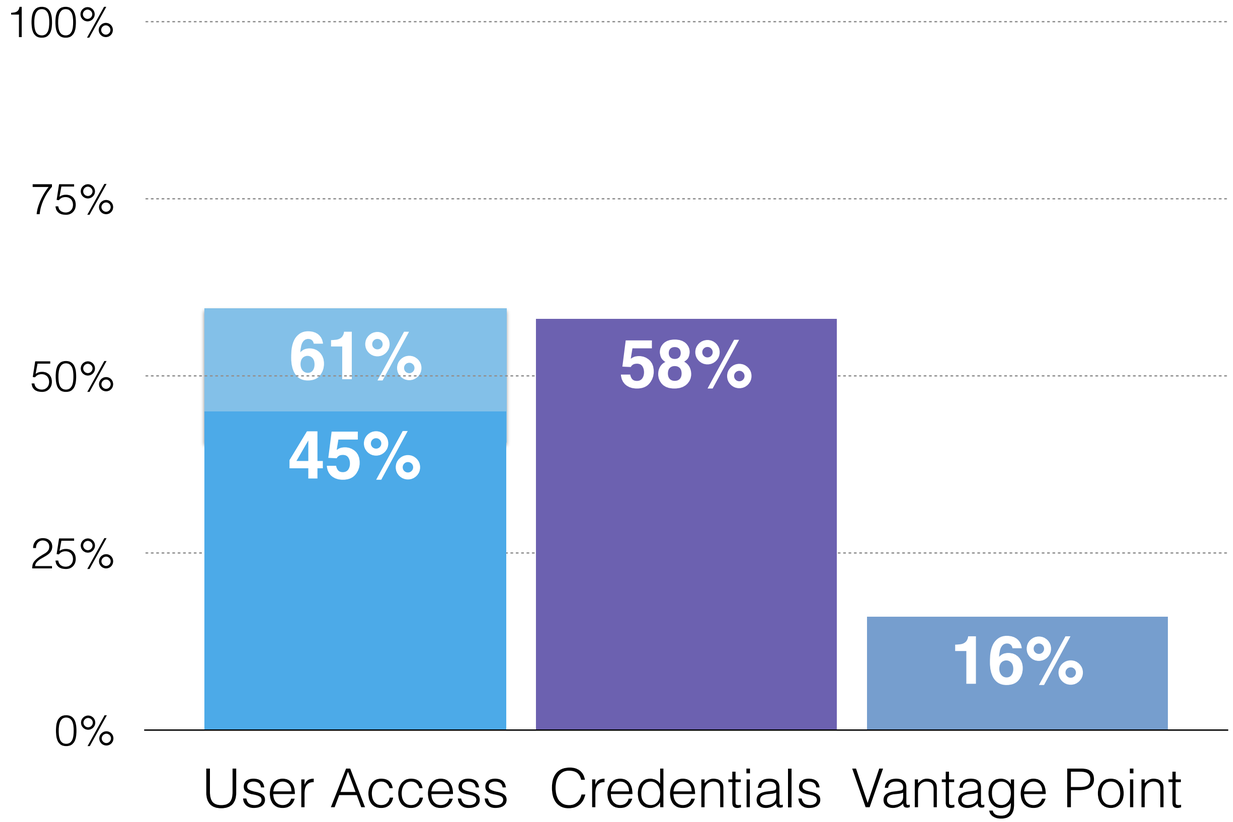


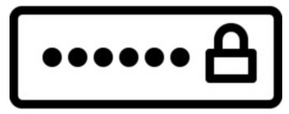


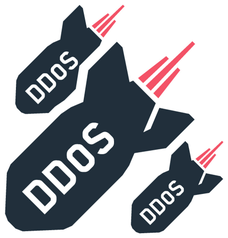
Overall Trends in Dataset

What **resource(s)** are RAT operators after?

- RATs are for user access
- RATs are easy, available
- RATs as “gateway”







Further Research Questions

Further Research Questions

Could realistic honeypots serve as a **tar-pit defense** against RAT campaigns?

Tarpit Defense

“[Consume] the attacker[’s] time and effort to no result.”

- *The Deception Toolkit*

Tarpit Defense

“[Consume] the attacker[’s] time and effort to no result.”

- The Deception Toolkit

- Average interaction: **4 minutes**
- Average remote desktop interaction: **7 minutes**
- **52.9** hours of interaction / **10,800** machine-hours

Tarpit Defense

“[Consume] the attacker[’s] time and effort to no result.”

- The Deception Toolkit

- Average interaction: **4 minutes**
- Average remote desktop interaction: **7 minutes**
- **52.9** hours of interaction / **10,800** machine-hours
- Honeypot realism cost-benefit

Conclusion

Conclusion

- Obtained and decoded **777** interactive sessions with DarkComet operators by executing malware in honeypots

Conclusion

- Obtained and decoded **777** interactive sessions with DarkComet operators by executing malware in honeypots
- Attackers seek access to the **victim user**, **credentials**, and **vantage points**

I have…a personal laptop. I put a piece of tape over the camera.

- James Comey
(former) FBI Director

Conclusion

- Obtained and decoded **777** interactive sessions with DarkComet operators by executing malware in honeypots
- Attackers seek access to the **victim user**, **credentials**, and **vantage points**
- RATs enable, encourage **amateur "hackers"** to cause serious harm to individuals online
  - We show operator Op-Sec is terrible
  - Inexpensive honeypots gather attribution information
  - Law enforcement could use this same technique

I have…a personal laptop. I put a piece of tape over the camera.

- James Comey
(former) FBI Director

"Law enforcement confirms that RATs…are a growing problem."

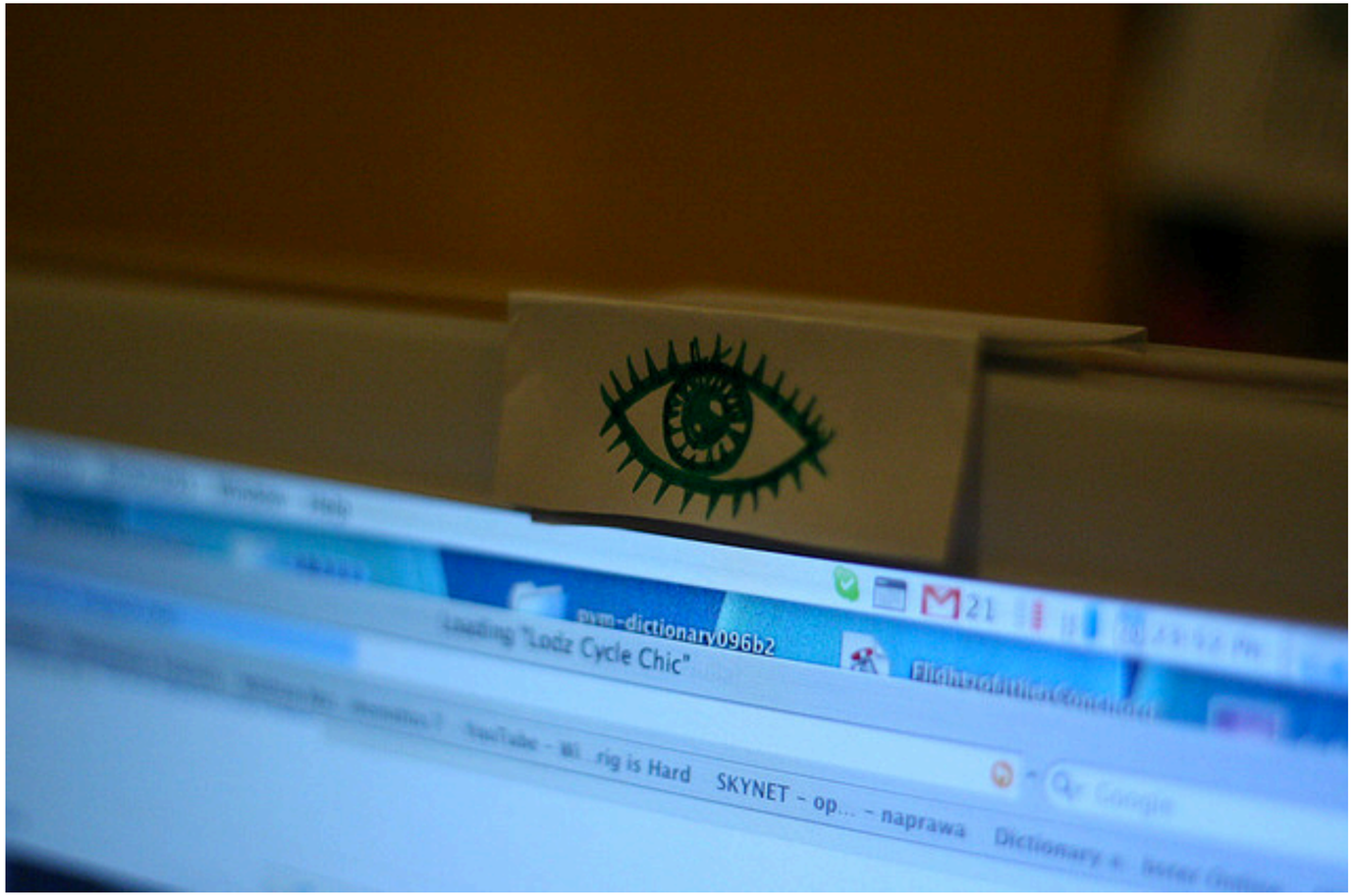
- Digital Citizens Alliance

Questions?

Brown Farinholt

UC San Diego

bfarinho@cs.ucsd.edu



Backup Slides

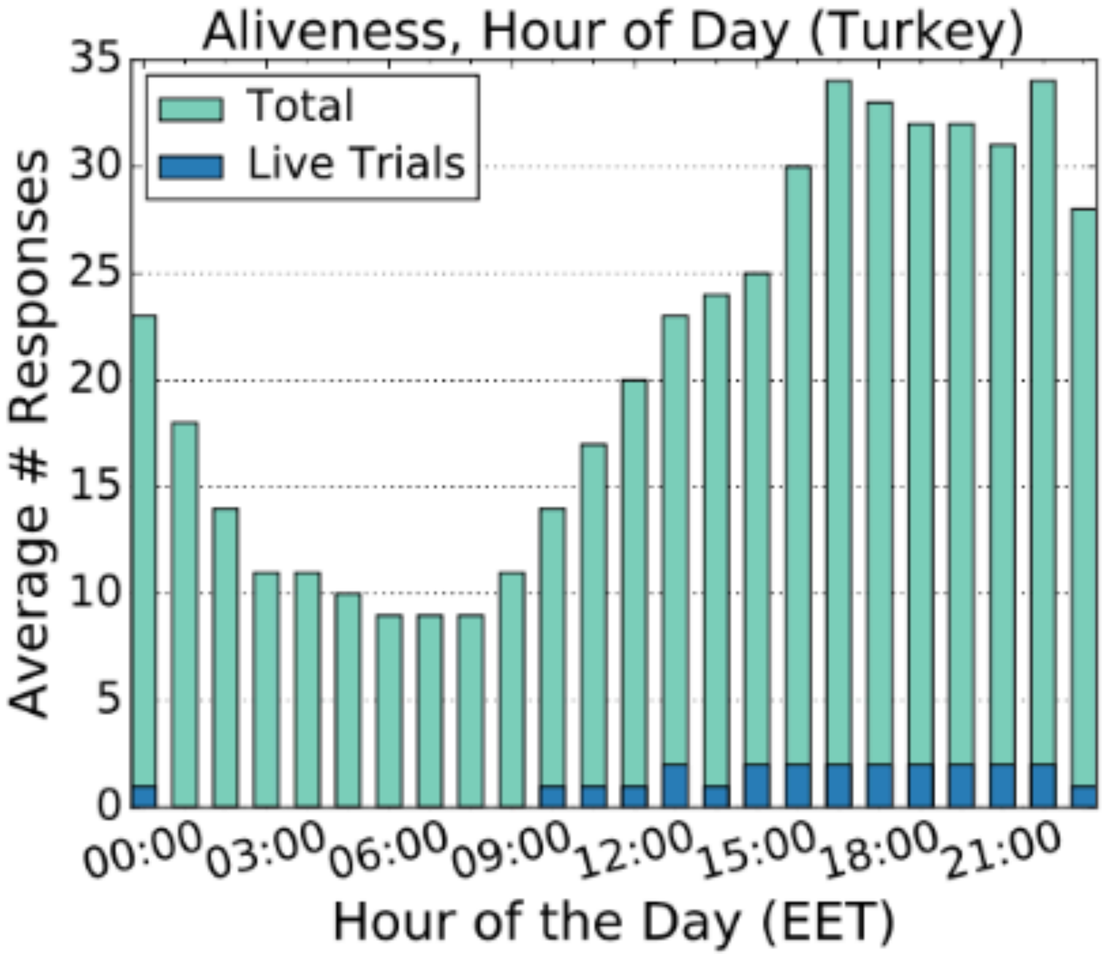
Operator OpSec is Terrible

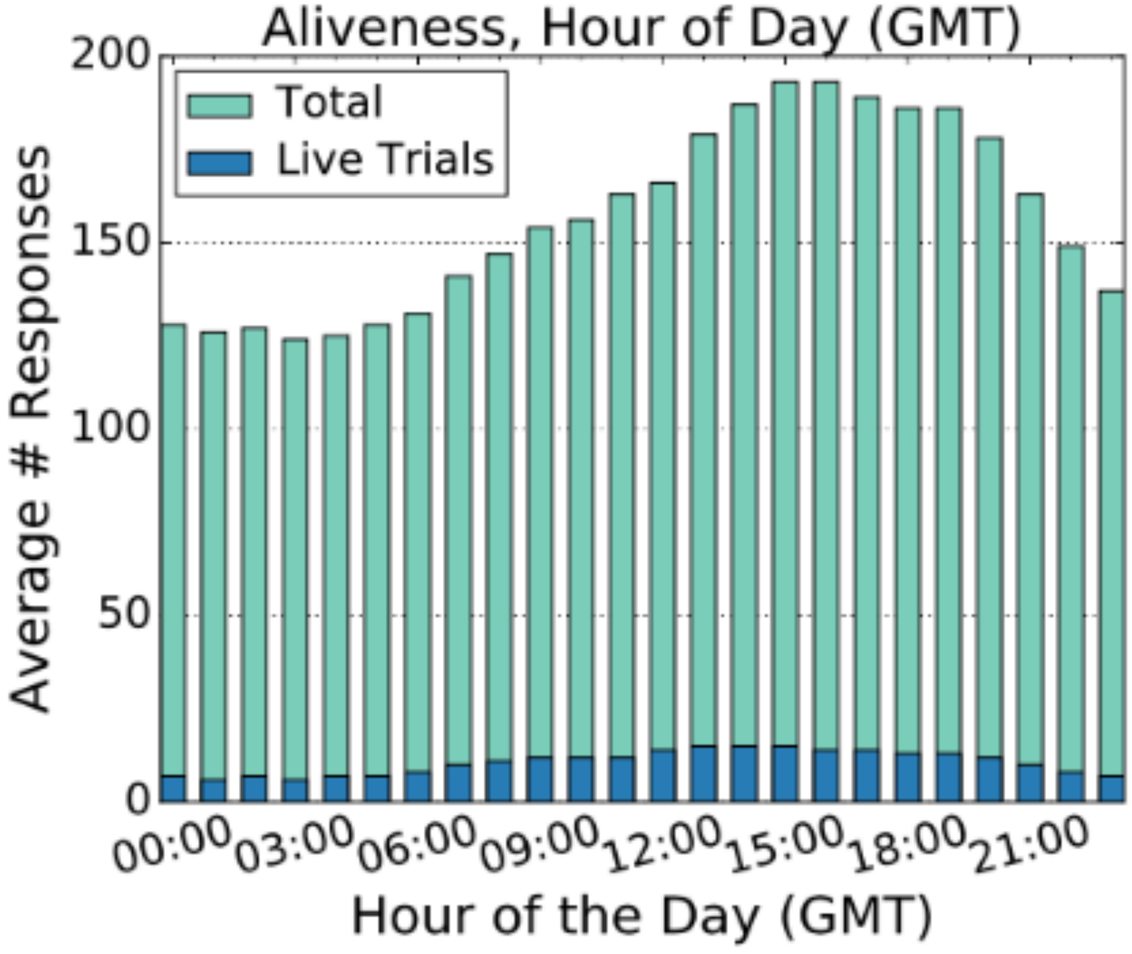
- 90% of operator IP addresses are **residential** and static
- Attackers often make **no effort to check** if the machine is a honeypot, engage in illegal activity immediately
- Some operators revealed **PII** (which we discarded, IRB) in an attempt to coax us (the victims) into communicating with them
- Some operators visited, even logged into their **personal accounts** in our machines

Related Work

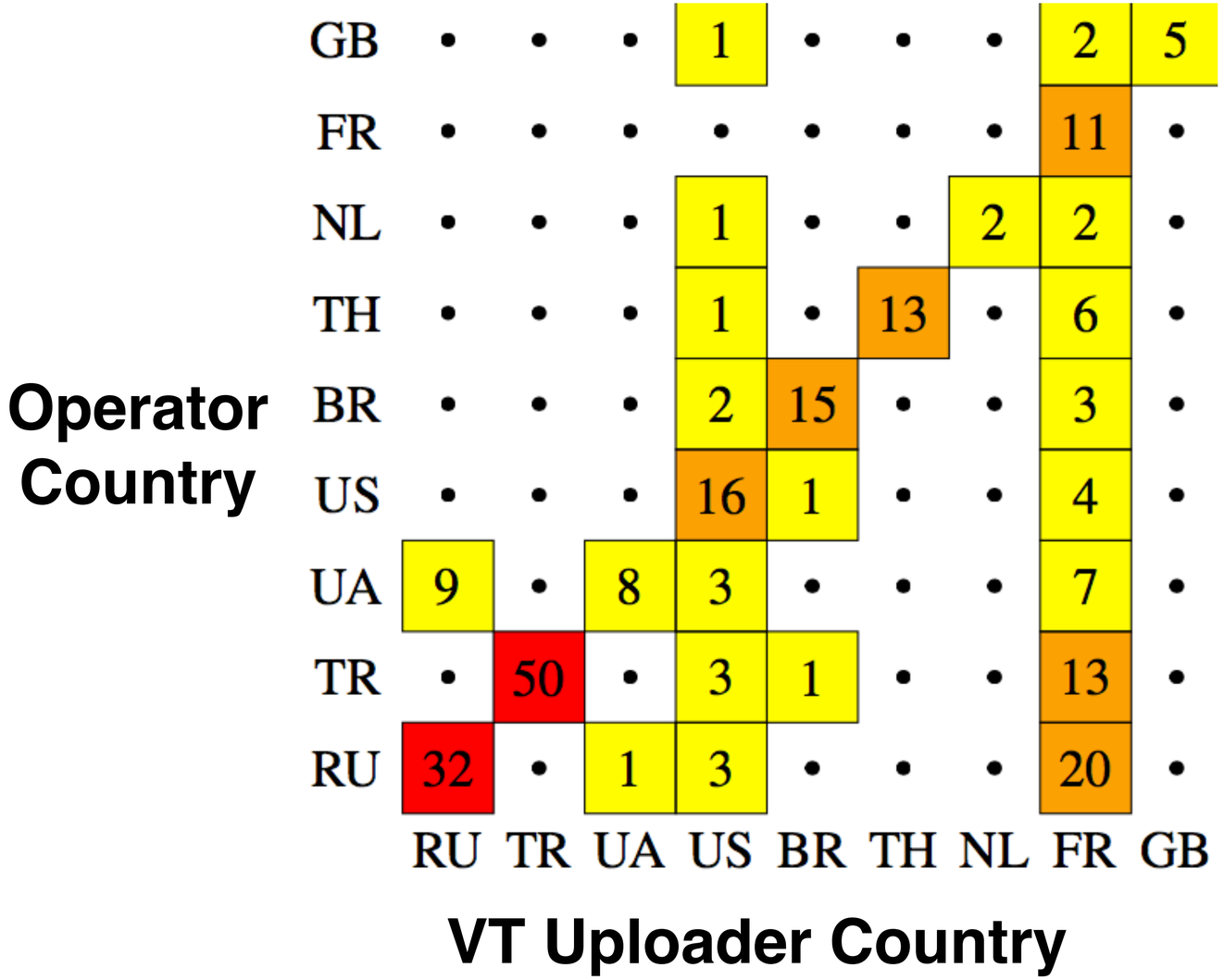
- Honeypots:
  - C. Stoll - *The cuckoo's egg*
- Low-volume RAT attacks in the wild:
  - Marczak et al. - *When governments hack opponents: A look at actors and technology.*
- RAT criminal community:
  - Digital Citizens Alliance - "*Selling slaving*"

What is a diurnal pattern?





Victim vs Operator Country



Further Research Questions

Could realistic honeypots serve as a **tar-pit defense** against RAT campaigns?

Further Research Questions

Could realistic honeypots serve as a **tar-pit defense** against RAT campaigns?

Do RAT operators unwittingly give up **threat intelligence** in compromised systems?

Threat Intelligence

Threat Intelligence: Technical indicators about threats that can inform defenses and/or identify actors and infrastructure

Threat Intelligence

Threat Intelligence: Technical indicators about threats that can inform defenses and/or identify actors and infrastructure

Attackers…

- Visited **123** URLs
- Dropped **34** executables
- Used **13** different honey-credentials offline
- Offered **PII**, used **ACTUAL CREDENTIALS**

Threat Intelligence

Threat Intelligence: Technical indicators about threats that can inform defenses and/or identify actors and infrastructure

Attackers…

- Visited **123** URLs
- Dropped **34** executables
- Used **13** different honey-credentials offline
- Offered **PII**, used **ACTUAL CREDENTIALS**

} **Attack Attribution**