



# To Catch a Ratter:

## Monitoring the Behavior of Amateur DarkComet RAT Operators in the Wild

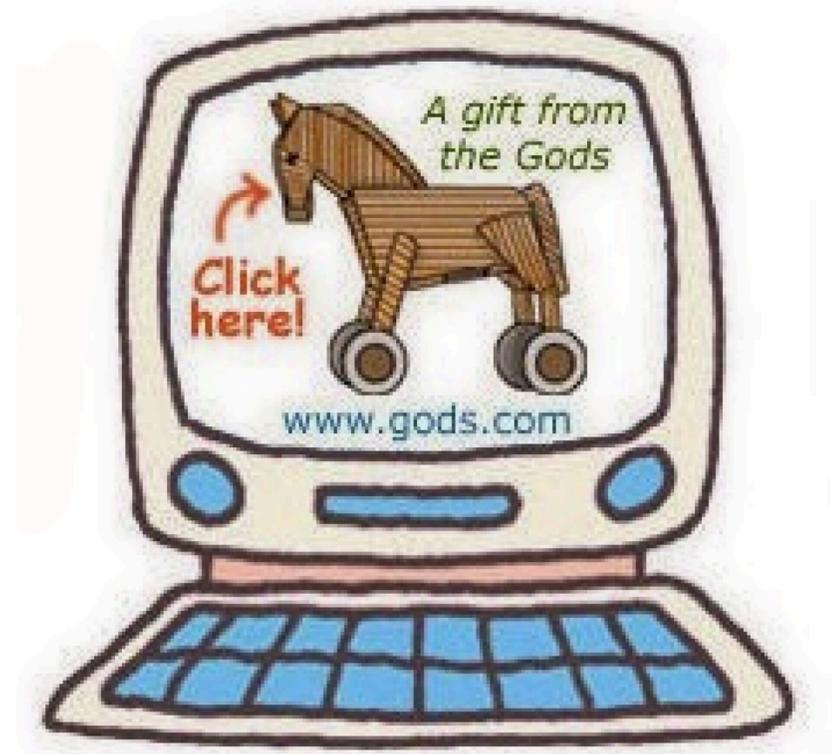
**Brown Farinholt**, Haikuo Yin, Kirill Levchenko  
Mohammad Rezaeirad  
Paul Pearce  
Hitesh Dharmdasani  
Stevens Le Blond  
Damon McCoy

UC San Diego  
George Mason University  
UC Berkeley  
Informant Networks  
EPFL & MPI-SWS  
New York University



# 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



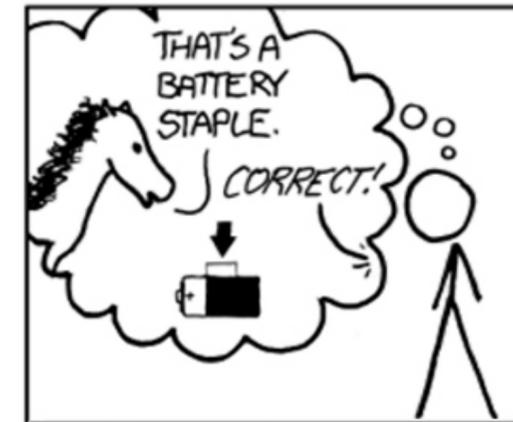
Chat Client



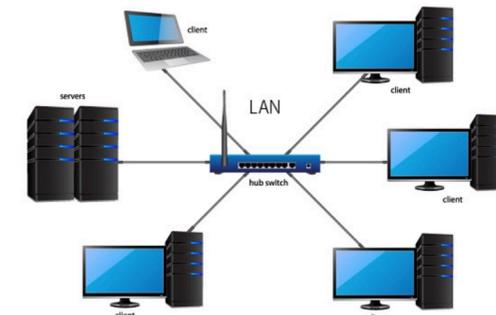
Remote Desktop



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/)  
[https://www.reddit.com/r/.../how\\_to\\_setup\\_dark\\_comet\\_rat\\_with\\_download\\_and/](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=58kSMFoINys>  
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 ...](http://www.mediafire.com/file/84sxnqfh1c78wy5/DarkComet_5.3.1...)

### How To Setup DarkComet R.A.T Be Successful 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

The screenshot shows the Hack Forums website interface. At the top, there's a navigation bar with links: Home, Upgrade, Search, Members, Extras, Wiki, Help, Follow, Contact. Below that, a user greeting says "Welcome back, [redacted]" with links for "View New Posts", "Your Threads", "Your Posts", and "Private Messages (Unread 0, Total 1)". There's also a link for "Open Buddy List".

The main content area is titled "Hack Forums / Search / Results". It shows a list of search results with columns for Thread / Author, Forum, Replies, and Last Post [asc].

Thread / Author	Forum	Replies	Last Post [asc]
[TUT] DarkComet v3.0 to v3.2 setup, step by step, pictures + video [Noob Friendly] ( 1 2 3 4 ... 86 ) MyStErIoUs-87	Hacking Tutorials	855	09-20-2016 02:14 PM Last Post: peno
(TUTORIAL) How to Setup Darkcomet RAT 5.3.1 ~ [FULL BEGINNERS Guide to DarkComet] ( 1 2 3 4 ... 69 ) Orochimaru	Hacking Tutorials	683	09-20-2016 02:07 PM Last Post: peno
[Exploit] Hack DarkComet users just with IP! ( 1 2 3 4 ... 9 ) Slayer616	Remote Administration Tools	86	09-07-2016 02:15 AM Last Post: Brinoz
[TUT] DarkComet RAT v3.0 Setup + DarkComet Crypter v1.0.0 ( 1 2 ) TdC	Hacking Tutorials	11	08-23-2016 03:29 PM Last Post: Bugato
New to DarkComet, my darkcomet server doesnt show up in users tab? ( 1 2 3 ) KillerSSJ8	Worms, Malware, and Viruses	23	08-18-2016 12:37 PM Last Post: phantom-ph
DarkComet Crypter 100% FUD Runtime + Scantime SUPPORTING RES AND EOF ! ( 1 2 3 4 ... 21 ) Akureyri	Referrals	203	07-15-2016 12:27 PM Last Post: TheTwoSeerlooms
[DarkComet] RAT! [DarkComet] (Outdated) ( 1 2 ) Marijuana x	Hacking Tutorials	19	06-22-2016 12:02 PM Last Post: 5tack
ADD darkcomet server (slaves darkcomet) to slave computer startup ( 1 2 ) mahaprabhu.deom	Beginner Hacking	19	02-15-2016 07:54 AM Last Post: DarkHead34

# 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

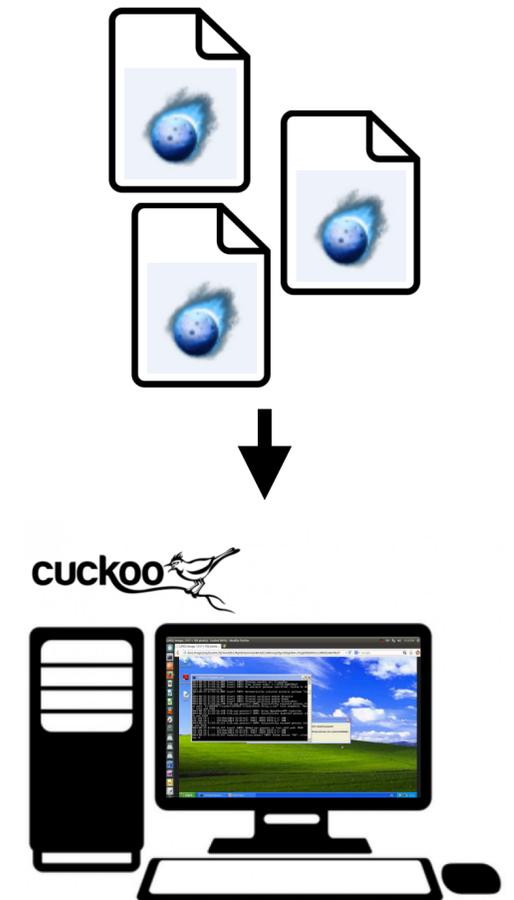
# The Plan

- Acquired **DarkComet RAT samples** from VirusTotal



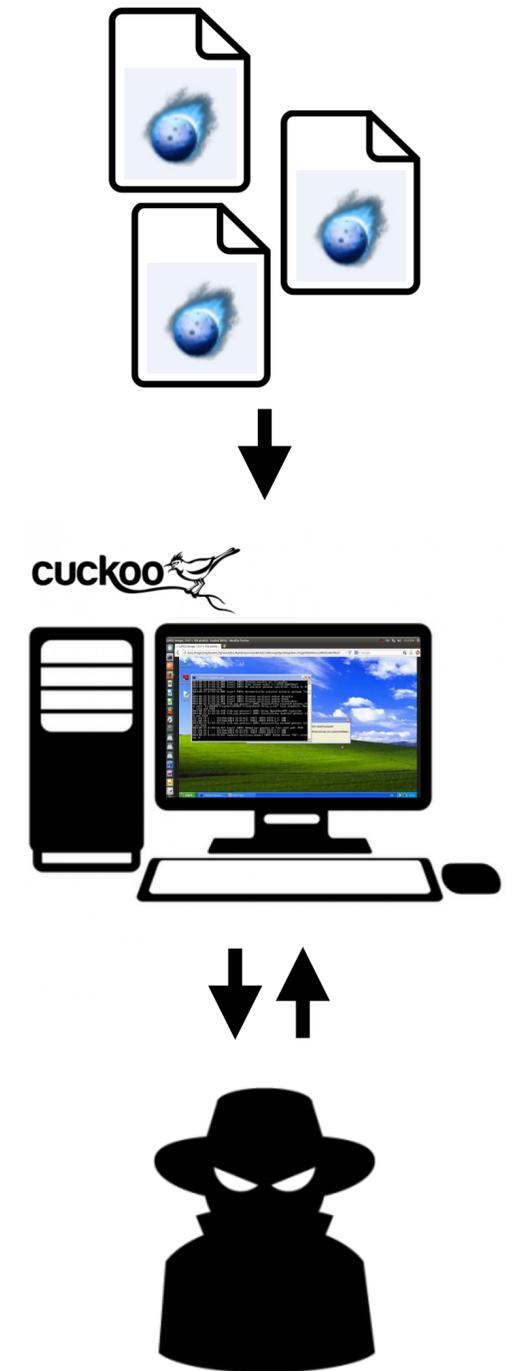
# The Plan

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



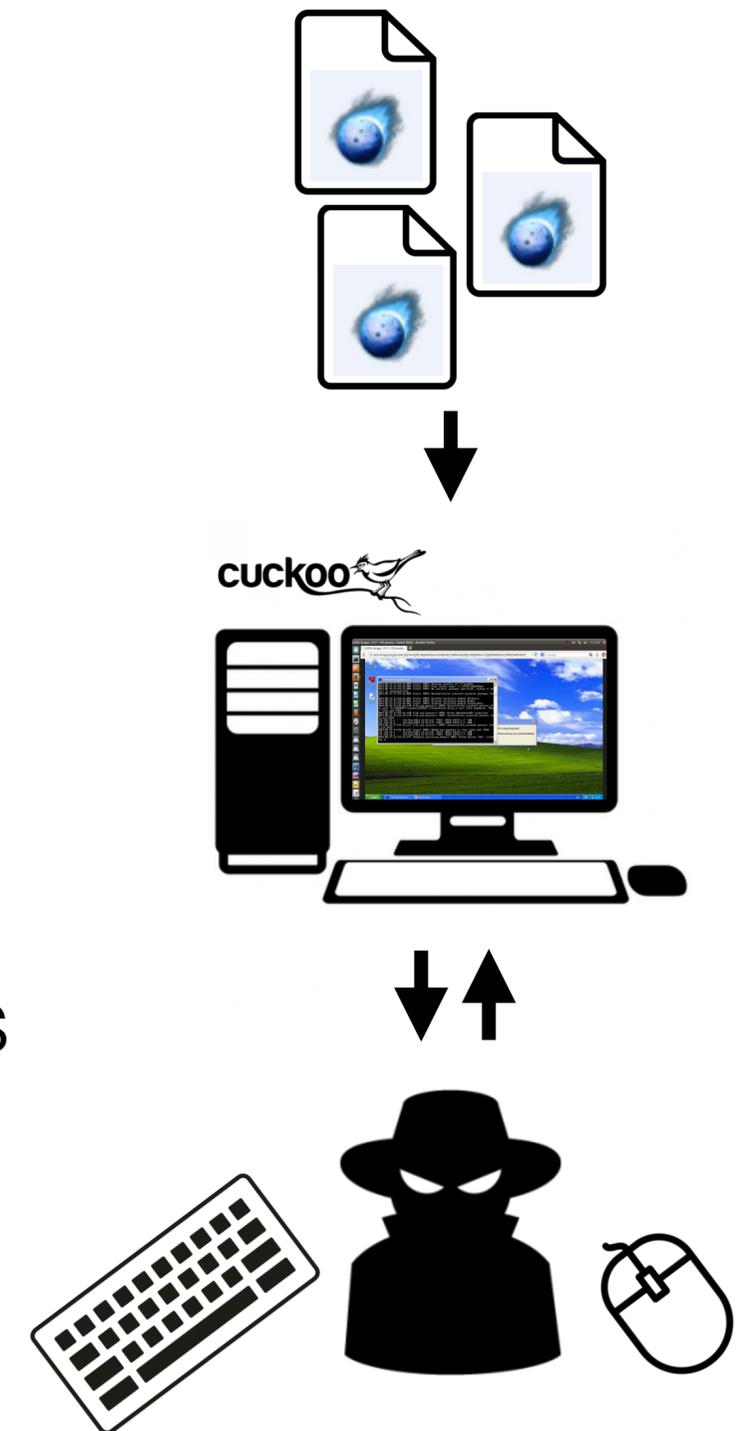
# The Plan

- 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

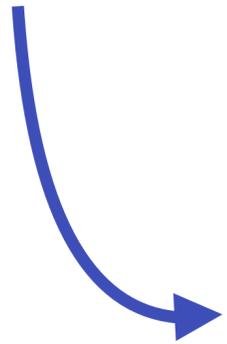


# Experiment

# Experiment



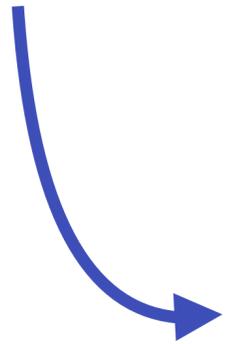
**19,109**  
samples



# Experiment



**19,109**  
samples



**13,339**  
addresses



# Experiment

 **virustotal**

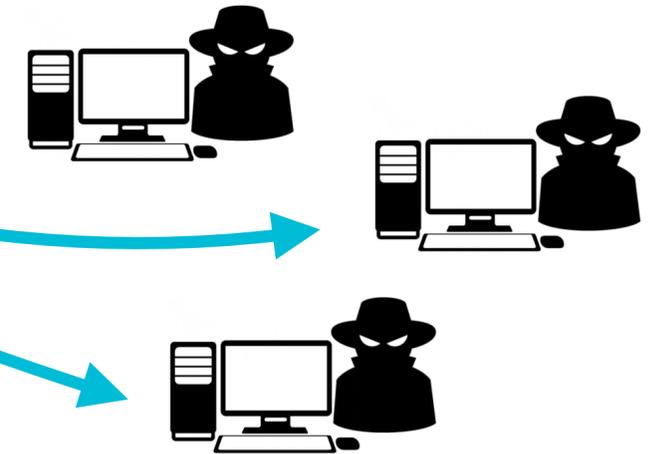
**19,109**  
samples



**13,339**  
addresses



**9,877**  
operators



# Experiment

 **virustotal**

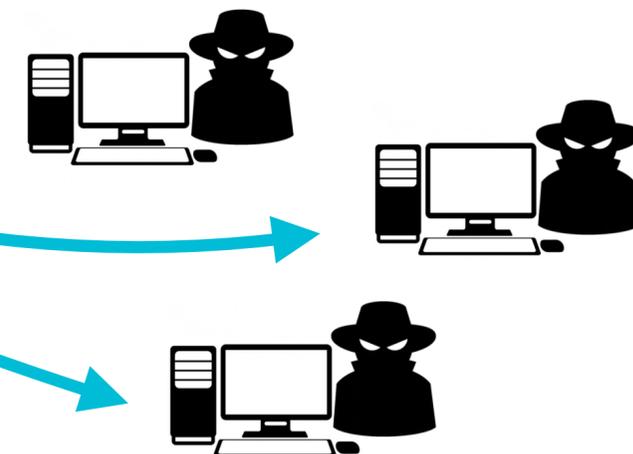
**19,109**  
samples



**13,339**  
addresses



**9,877**  
operators



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

# Experiment

 **virustotal**

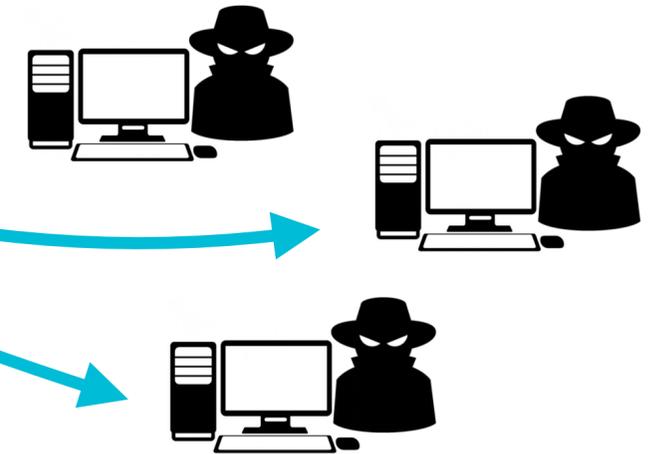
**19,109**  
samples



**13,339**  
addresses



**9,877**  
operators



# Experiment

 **virustotal**

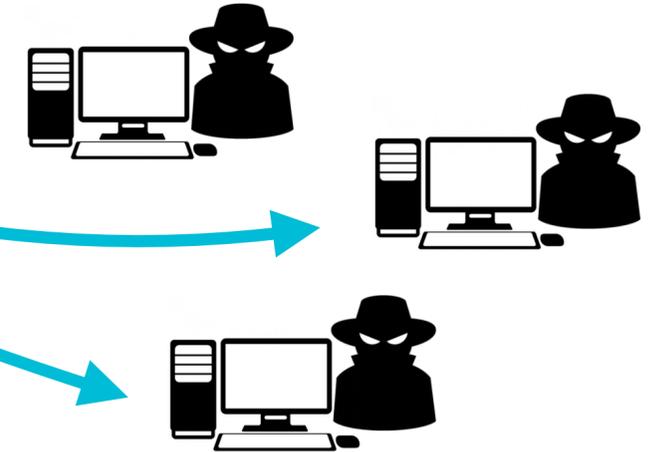
**19,109**  
samples



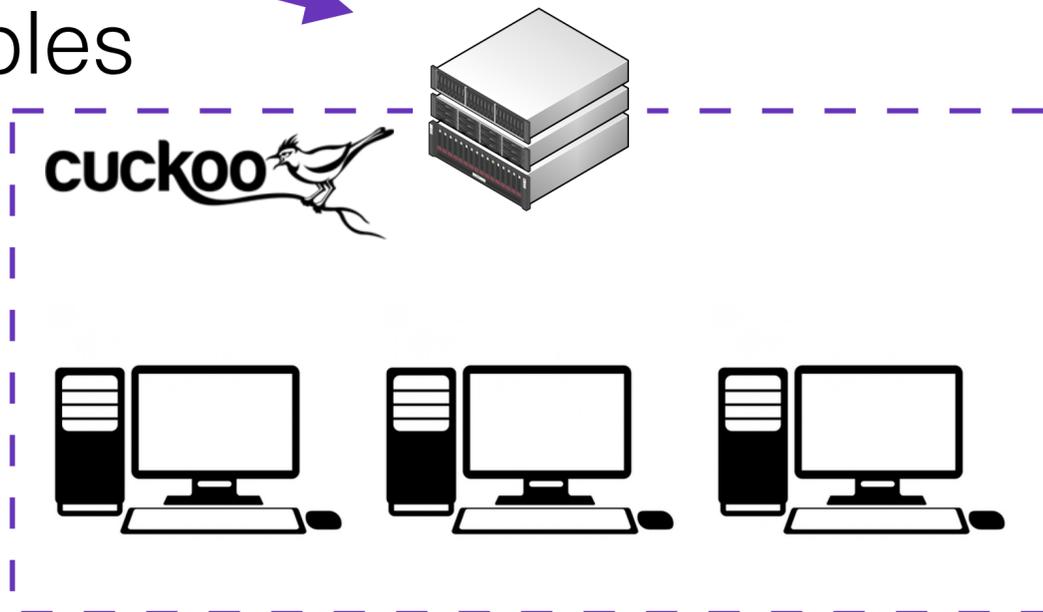
**13,339**  
addresses



**9,877**  
operators



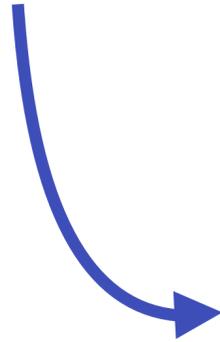
**1,165**  
live samples



# Experiment

virustotal

19,109  
samples



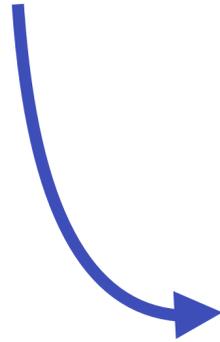
The screenshot shows a Windows desktop environment. The desktop background is a dark image of a space station. The taskbar at the bottom contains icons for Recycle Bin, File Explorer, Google Chrome, Mozilla Thunderbird, Notepad++, Steam, VLC media player, and Spotify. The desktop has several application icons: Recycle Bin, Pidgin, Git Shell, Acrobat Reader DC, PuTTY, FileZilla, Steam, GIMP 2, VLC media player, Google Chrome, WinRAR, LibreOffice 5.2, Spotify, Mozilla Thunderbird, Team Fortress 2, Notepad++, and GitHub. A GitHub pull request window is open, showing a list of pull requests for the 'research' repository. The selected pull request is 'Merge pull request #29 from jingzhehu/jh-fix-issue-22-rnn-unroll' by user 'espes'. The pull request details show a commit hash '1a437a9' and a list of files: 'models\conditional.py', 'models\layers.py', and 'models\transition.py'. A small icon of a person in a hat is visible on the right side of the desktop.



# Experiment

virustotal

19,109  
samples



**Applications**

Compare

master

Filter repositories

GitHub

- first\_paper
- research
- research-rootkit
- ResearchKit
- researchlei
- research\_public
- Other
- Tutorial

Merge pull request #29 from jingzhehu/jh-fix-issue-22-rnn-unroll  
7 days ago by espes

espes 1a437a9

fix issue #22

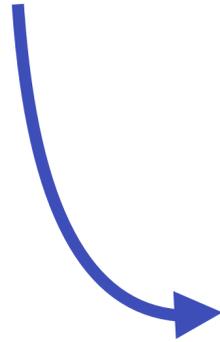
- models\conditional.py
- models\layers.py
- models\transition.py

3:07 PM  
10/17/2016

# Experiment

virustotal

19,109  
samples



**Applications**

**Filesystem**

Compare

Changes History

Pull request

Filter repositories

GitHub

first\_paper

research

research-rootkit

ResearchKit

researchlei

research\_public

Other

Merge pull request #29 from jingzhehu/jh-fix-issue-22-rnn-unroll

espes 1a437a9

fix issue #22

models\conditional.py

models\layers.py

models\transition.py

Merge pull request #29 from jingzhe... 7 days ago by espes

Merge pull request #26 from Yale323/patc... 24 days ago by George Hotz

Merge pull request #23 from zuijiawoniu/p... 1 month ago by George Hotz

Merge pull request #18 from rocfig/patch-2 2 months ago by espes

Merge pull request #16 from rocfig/patch-1 2 months ago by espes

Merge pull request #15 from solaris33/mas... 2 months ago by George Hotz

typos 2 months ago by George Hotz

Merge pull request #12 from rbiasini/patch-1 2 months ago by espes

Merge pull request #11 from commaai/Ede... 2 months ago by George Hotz

Merge pull request #10 from radarhere/pat... 2 months ago by espes

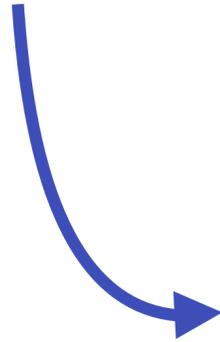
3:07 PM 10/17/2016



# Experiment

virustotal

19,109  
samples



Applications

Filesystem

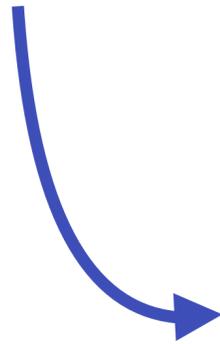
Browser History



# Experiment

virustotal

19,109  
samples



**Applications**

**Filesystem**

**Honey-Credentials**

**Browser History**

# Experiment

 **virustotal**

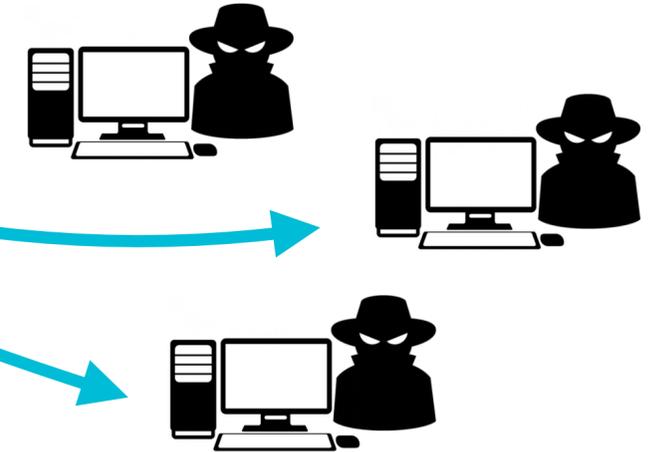
**19,109**  
samples



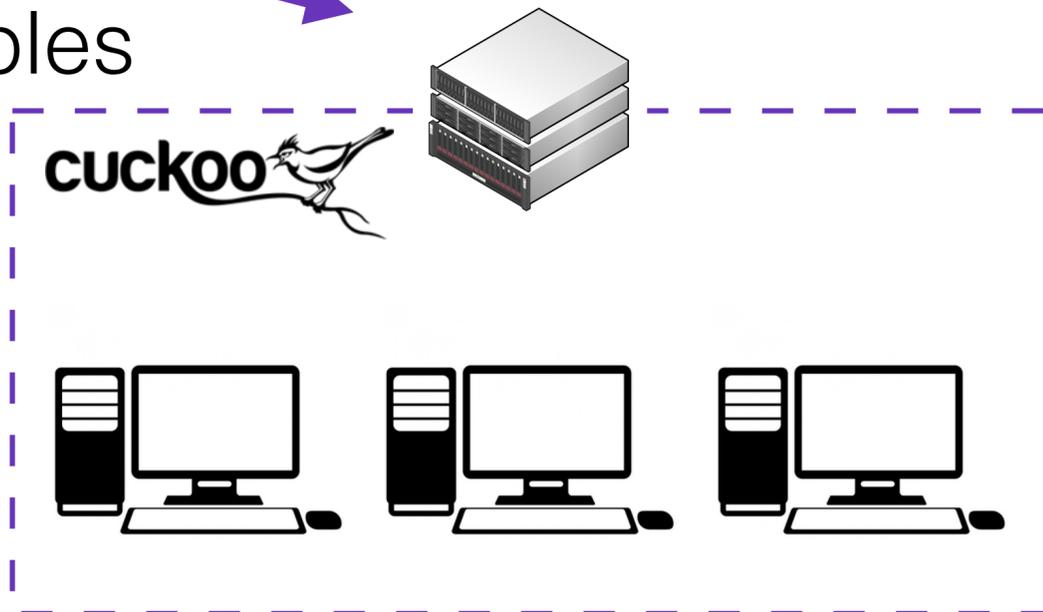
**13,339**  
addresses



**9,877**  
operators



**1,165**  
live samples



# Experiment

 **virustotal**

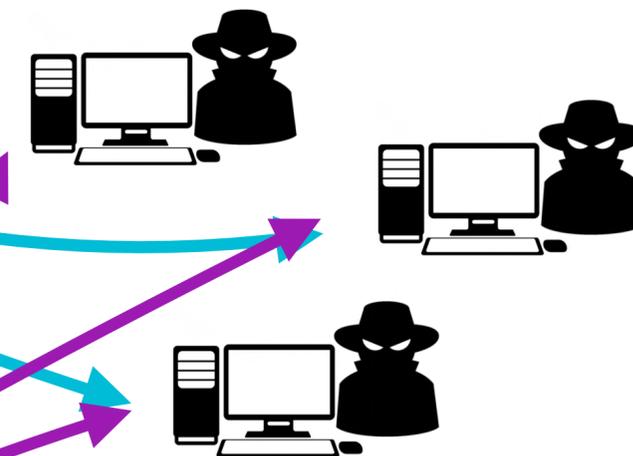
**19,109**  
samples



**13,339**  
addresses



**9,877**  
operators



**1,165**  
live samples

**cuckoo**



**777**  
interactions



4 Weeks

# Experiment



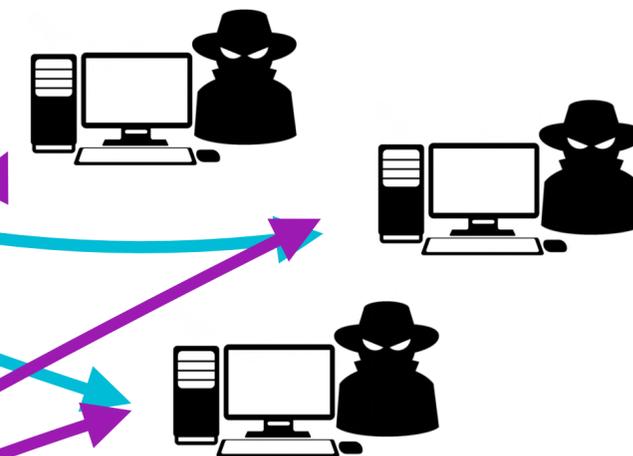
19,109  
samples



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**

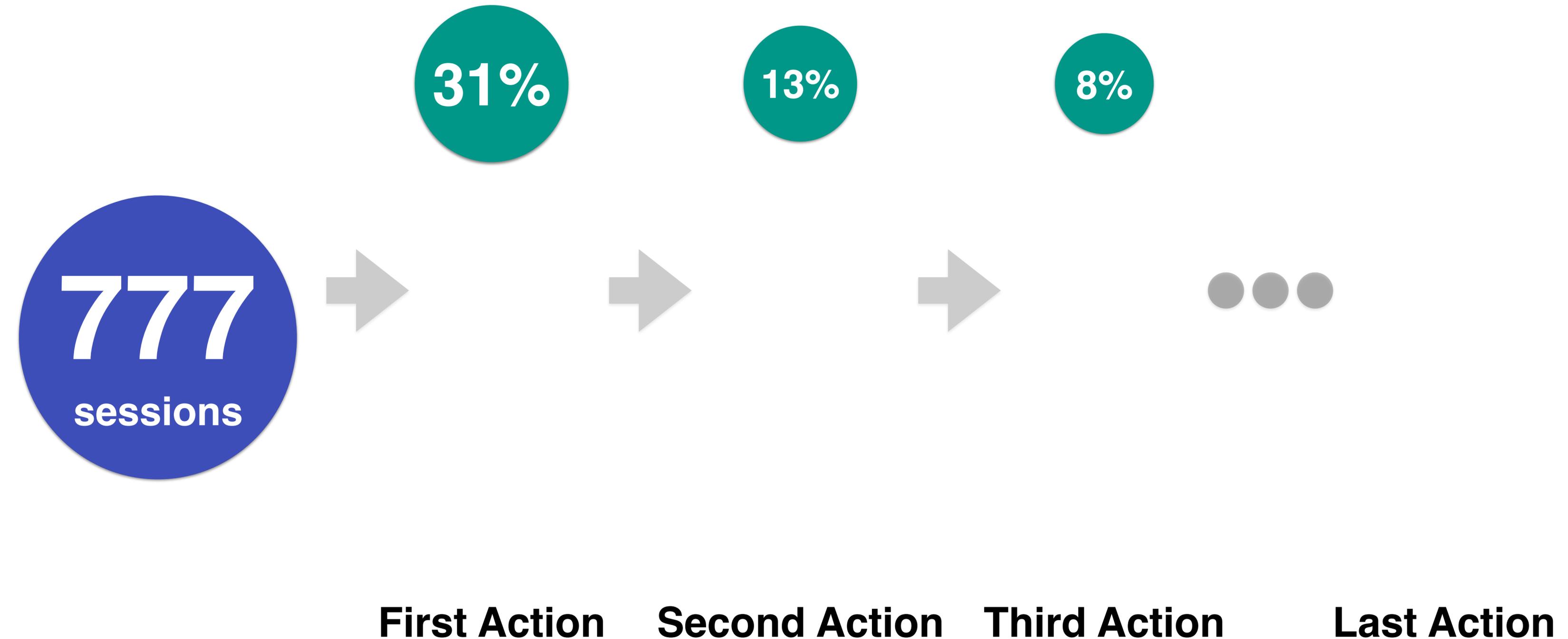
# Common Patterns of Action



**777**  
sessions

# Common Patterns of Action

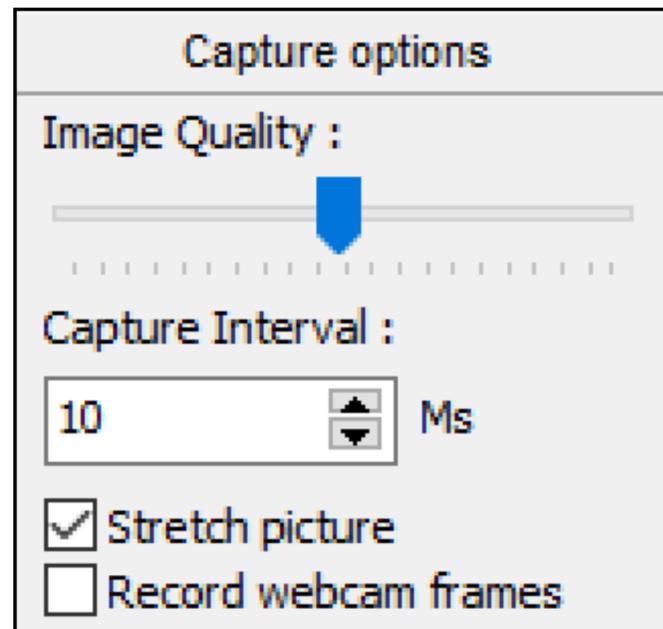
● Webcam, Audio



# (Attempted) User Monitoring

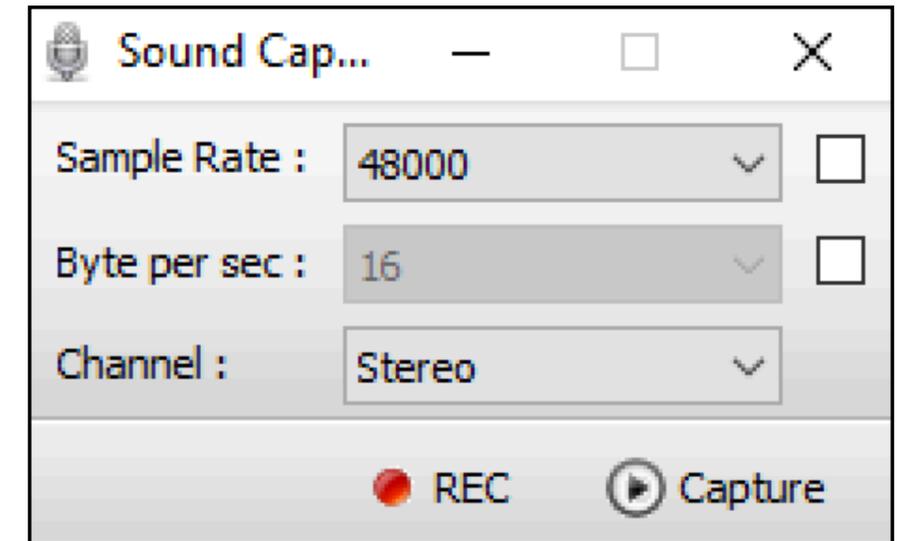
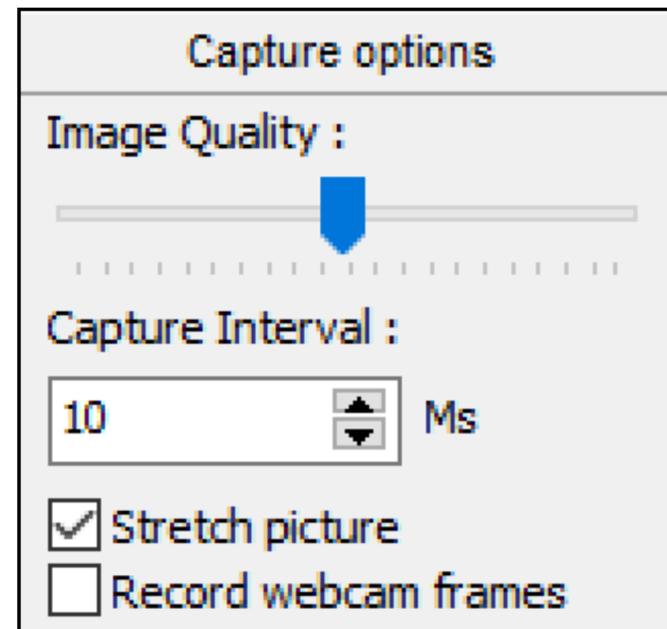


# (Attempted) User Monitoring



Webcam: **61%**

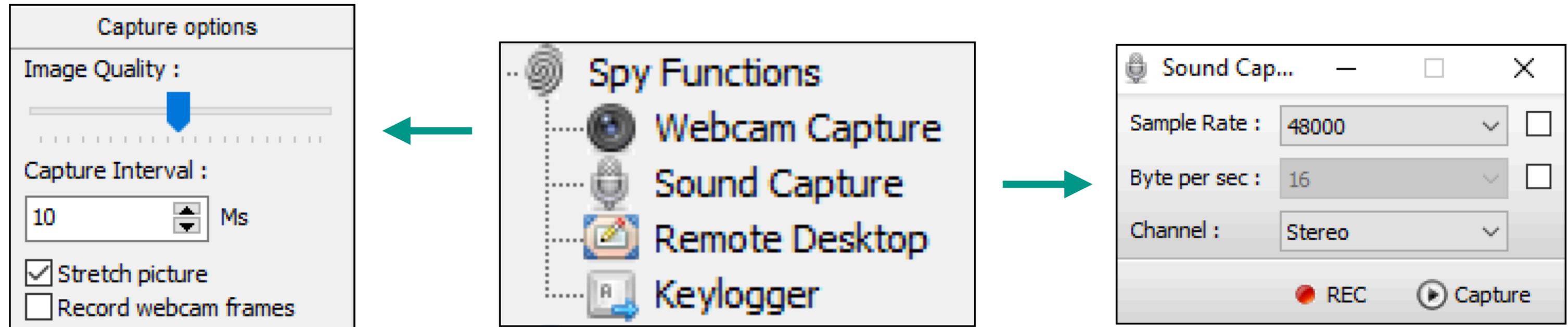
# (Attempted) User Monitoring



Webcam: **61%**

Microphone: **26%**

# (Attempted) User Monitoring



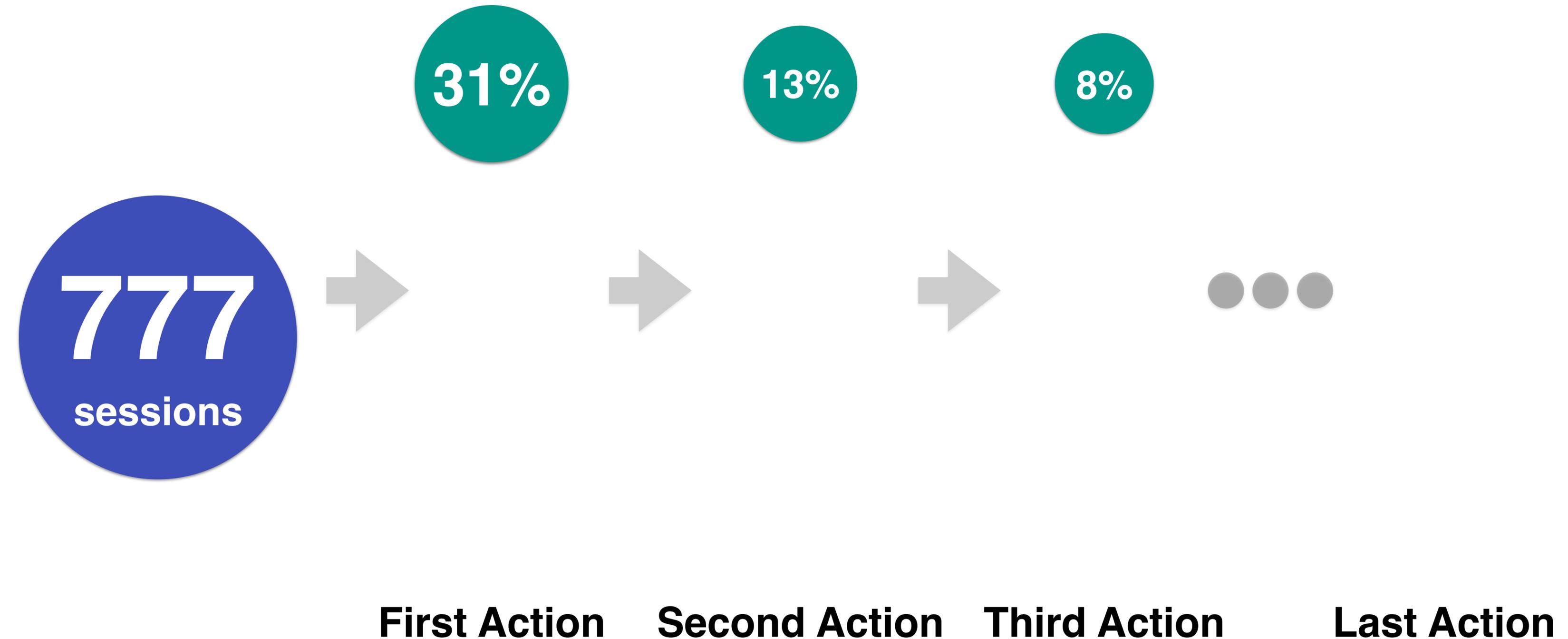
Webcam: **61%**

Microphone: **26%**

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

# Common Patterns of Action

● Webcam, Audio

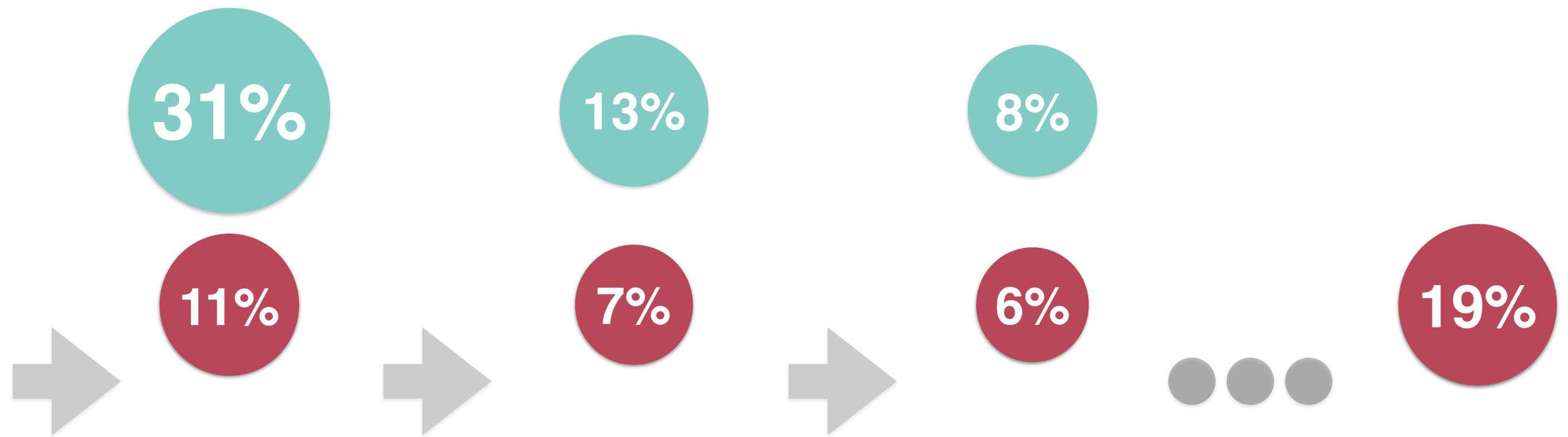


# Common Patterns of Action

● Webcam, Audio

● Passwords

777  
sessions



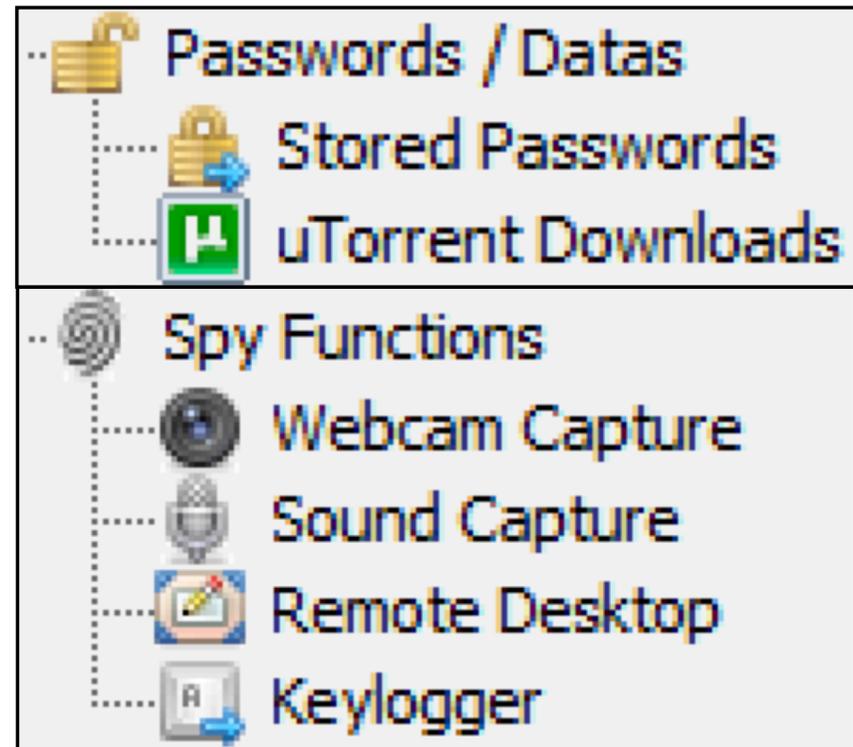
**First Action**

**Second Action**

**Third Action**

**Last Action**

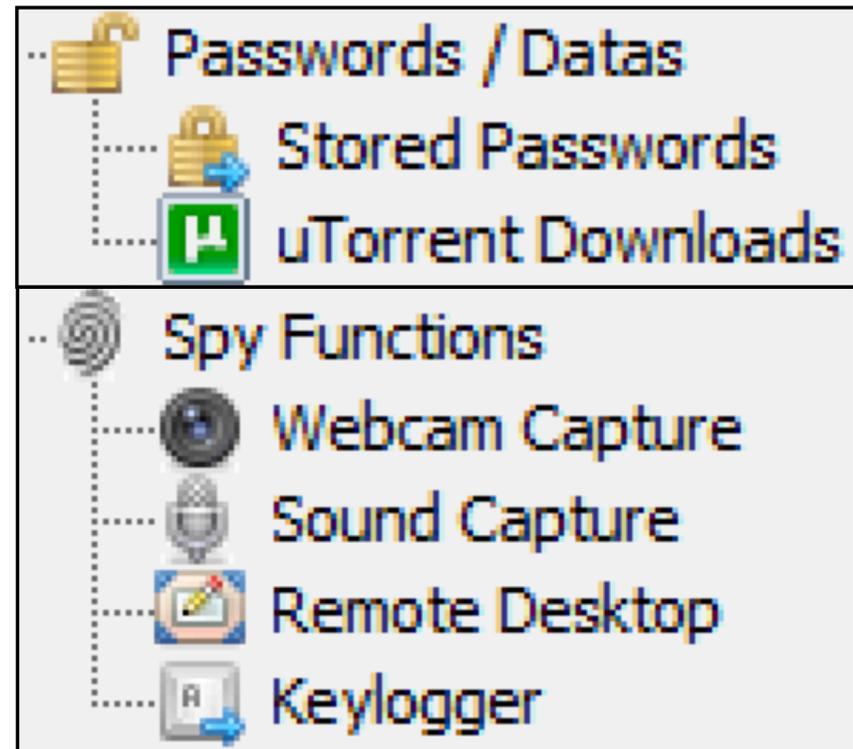
# Credential Theft



# Credential Theft

Stored Passwords : [DESKTOP-ENDE2HF / bfarinho], Socket : [15]

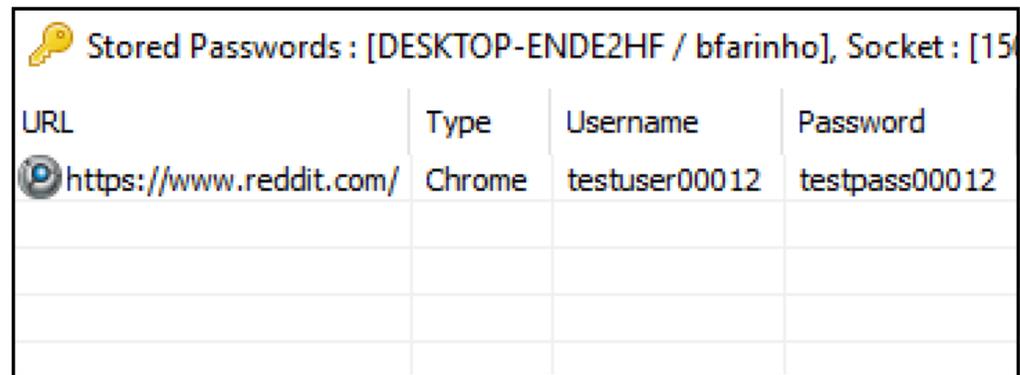
URL	Type	Username	Password
https://www.reddit.com/	Chrome	testuser00012	testpass00012



Passwords: **43%**

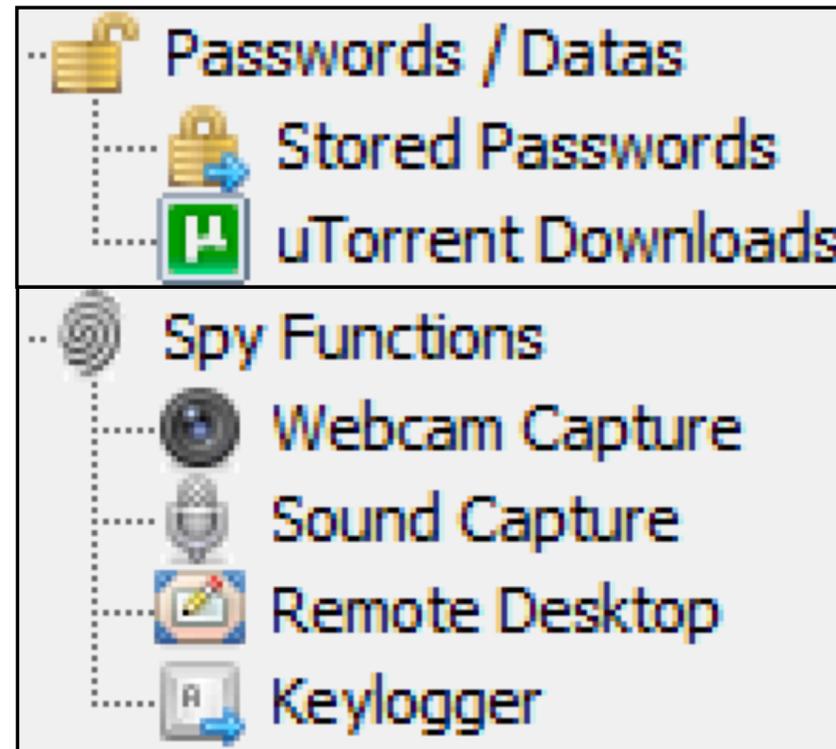
- Credentials seeded on honeypots were used **13** times outside study
- **Steam** (gaming platform) was probed often

# Credential Theft



URL	Type	Username	Password
https://www.reddit.com/	Chrome	testuser00012	testpass00012

Passwords: **43%**



Keylogger: **31%**

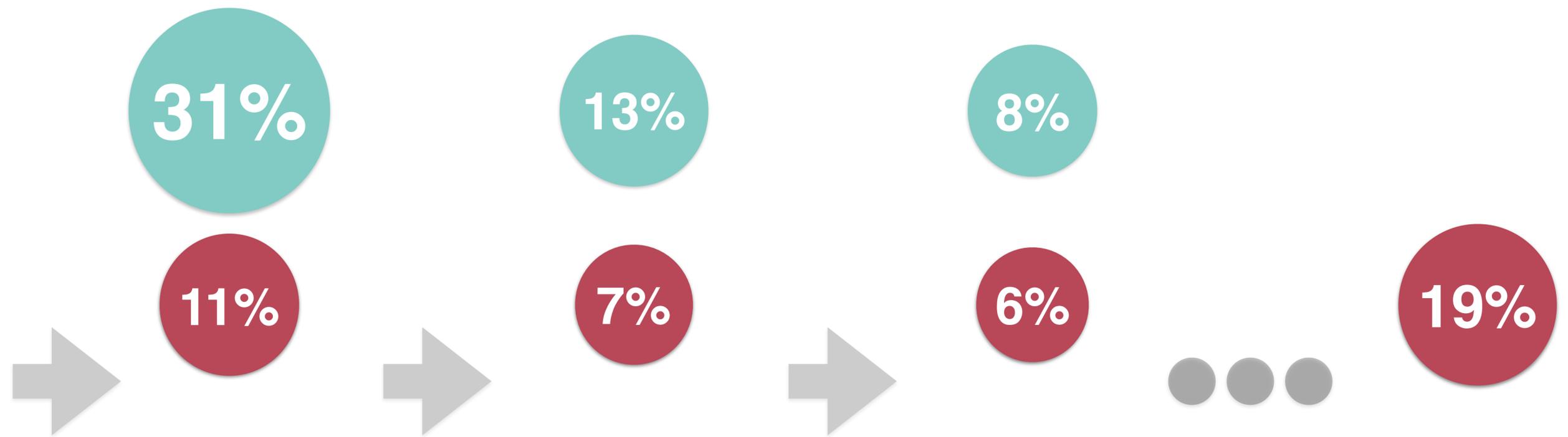
- Credentials seeded on honeypots were used **13** times outside study
- **Steam** (gaming platform) was probed often
- For one-click actions, these numbers are low... Recreational users?

# Common Patterns of Action

● Webcam, Audio

● Passwords

777  
sessions



**First Action**

**Second Action**

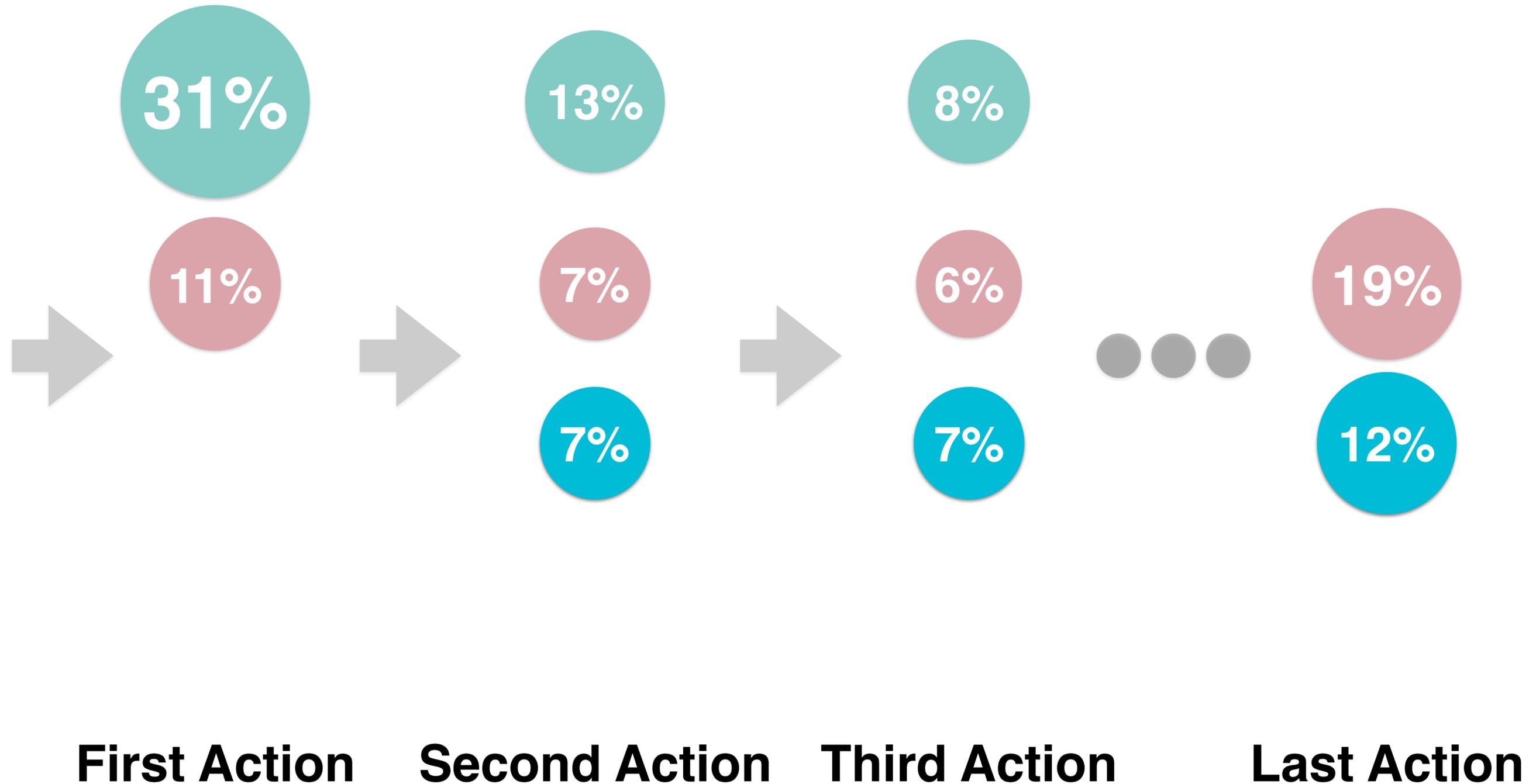
**Third Action**

**Last Action**

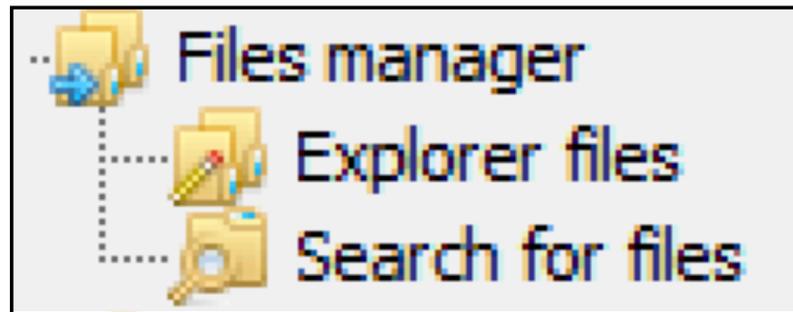
# Common Patterns of Action

- Webcam, Audio
- Passwords
- Filesystem

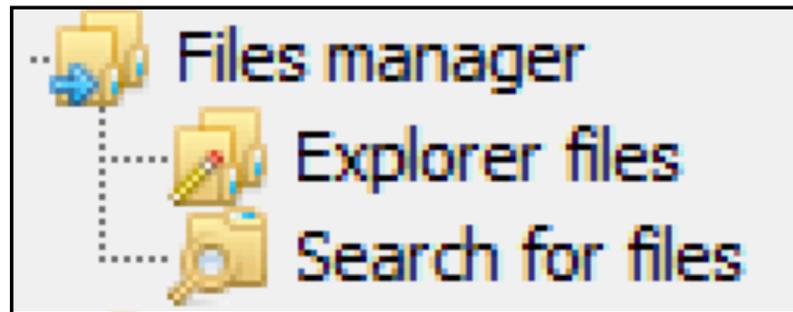
777  
sessions



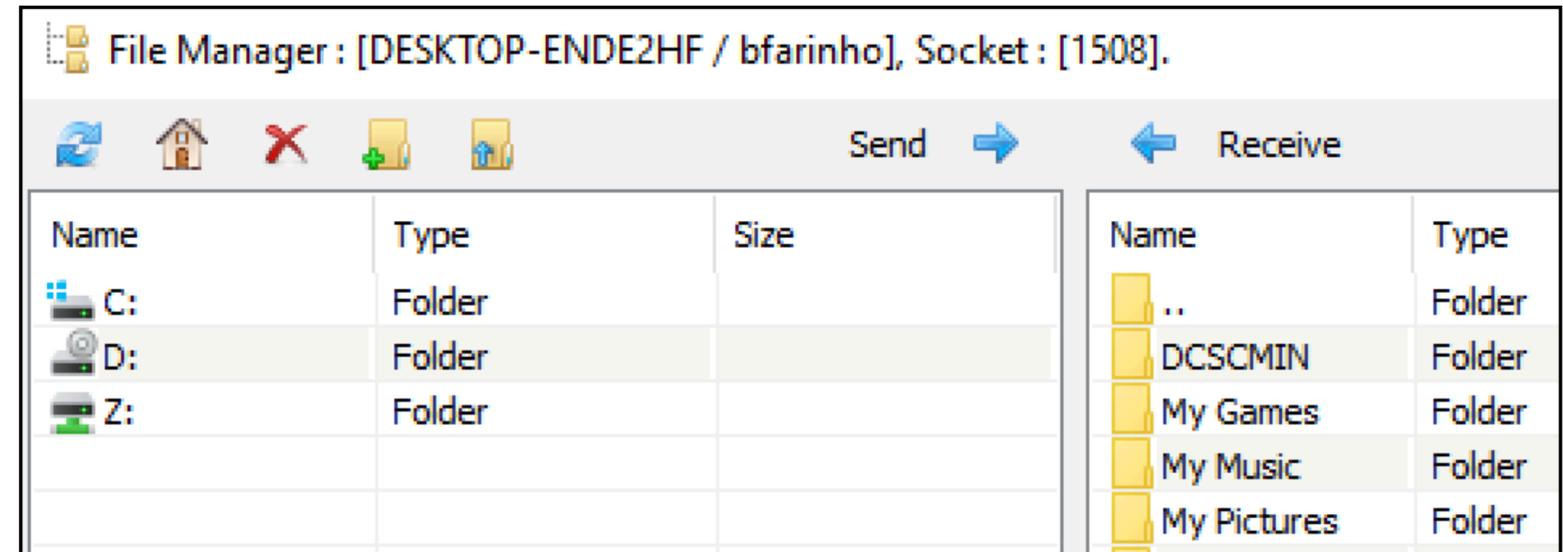
# Filesystem Access



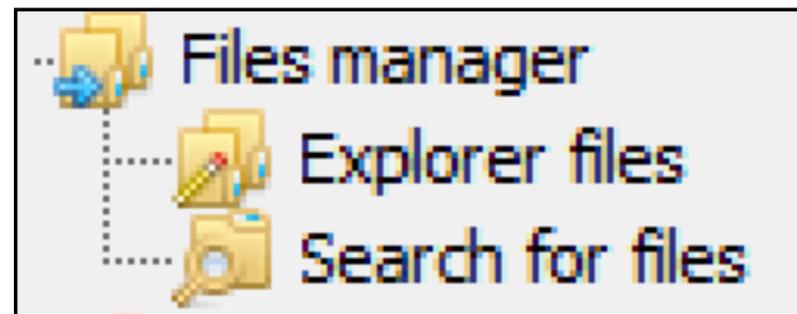
# Filesystem Access



Filesystem  
Exploration: **40%**

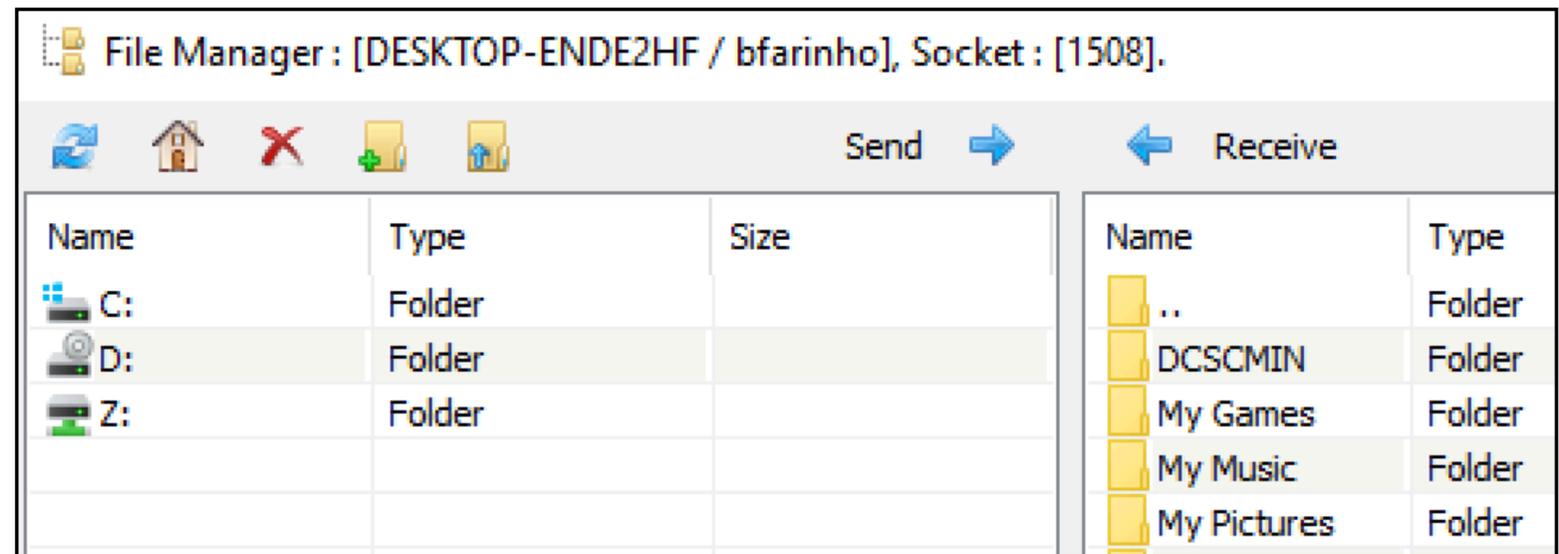


# Filesystem Access



Filesystem

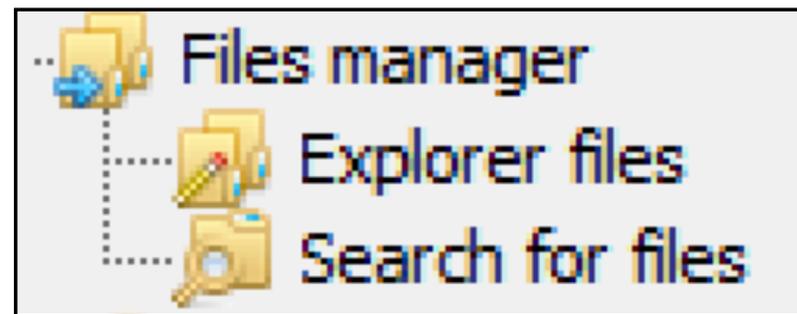
Exploration: **40%**



Upload: **18%**

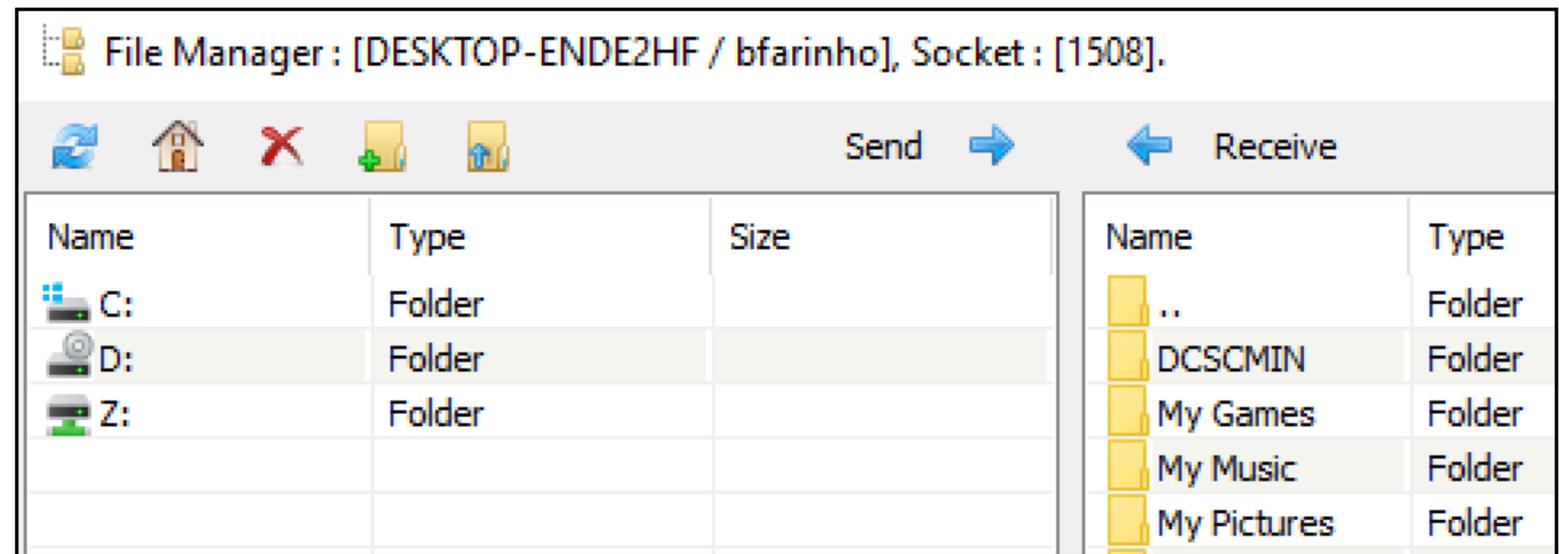
- **4%** of attackers uploaded hacking tools
- **34** unique executables uploaded, **19** new to VirusTotal

# Filesystem Access



Filesystem

Exploration: **40%**



Upload: **18%**

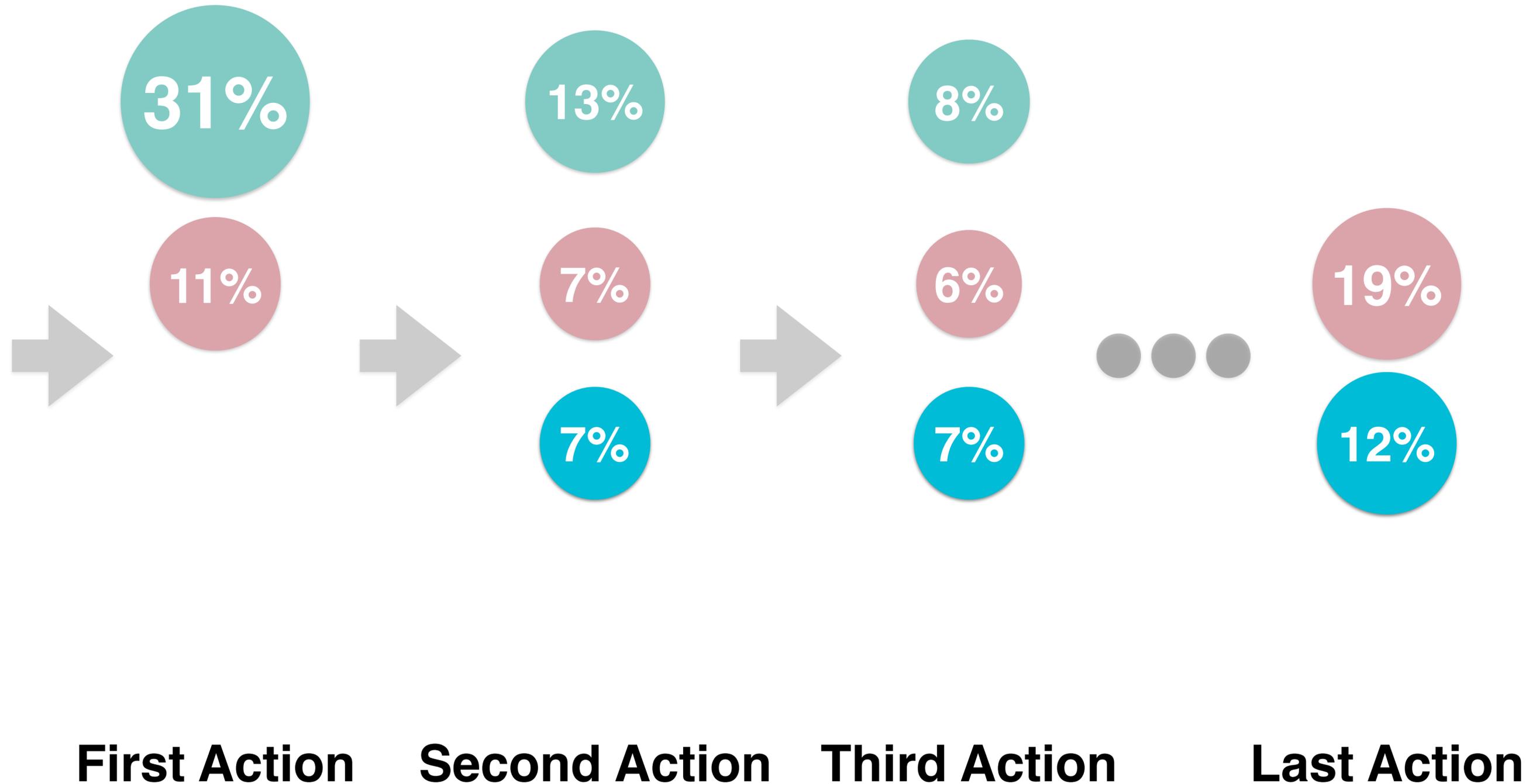
Download: **8%**

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

# Common Patterns of Action

- Webcam, Audio
- Passwords
- Filesystem

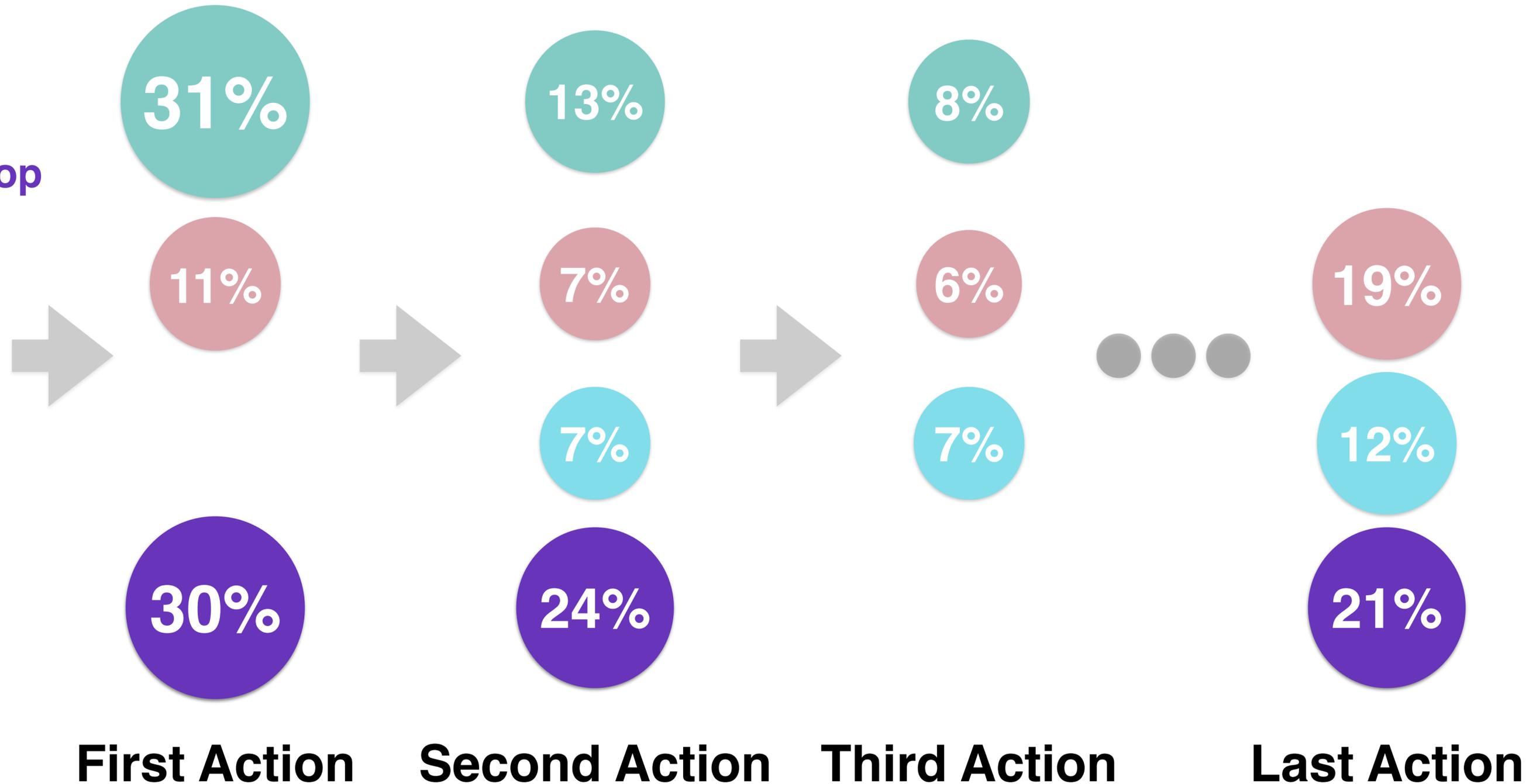
777  
sessions



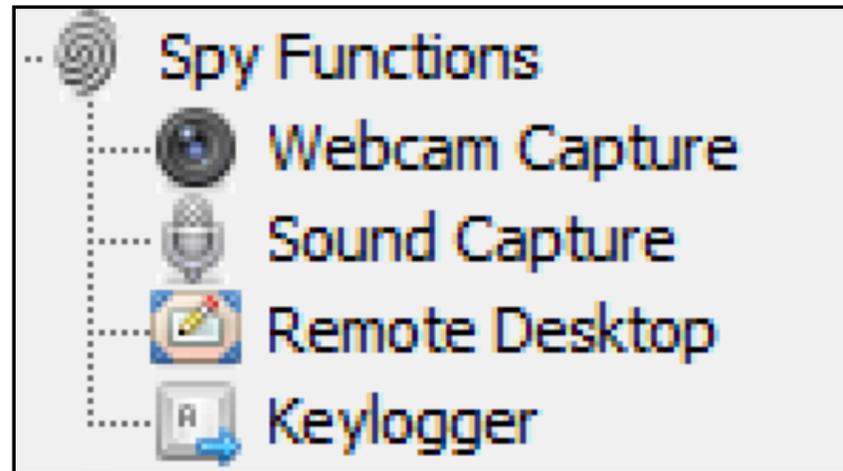
# Common Patterns of Action

- Webcam, Audio
- Passwords
- Filesystem
- Remote Desktop

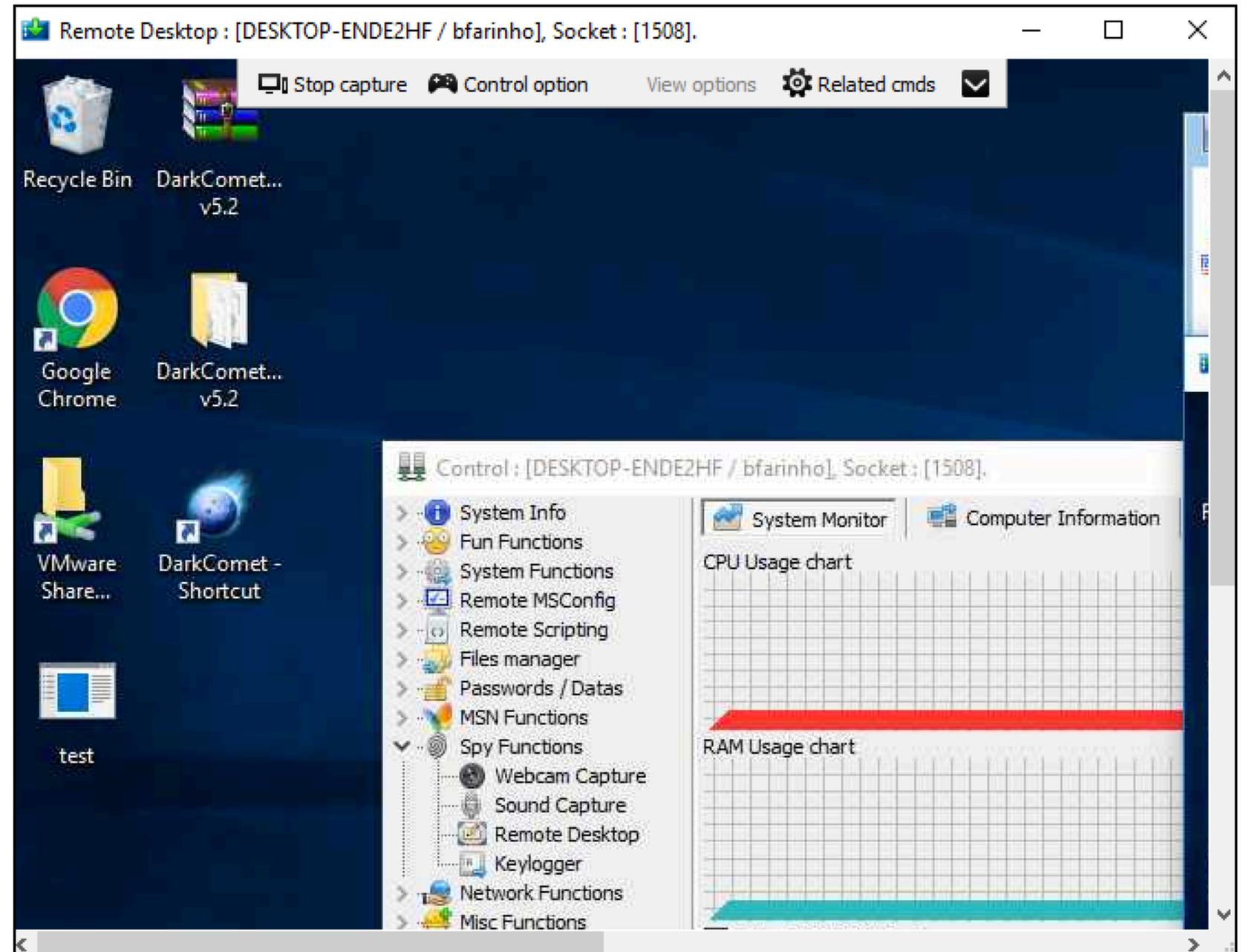
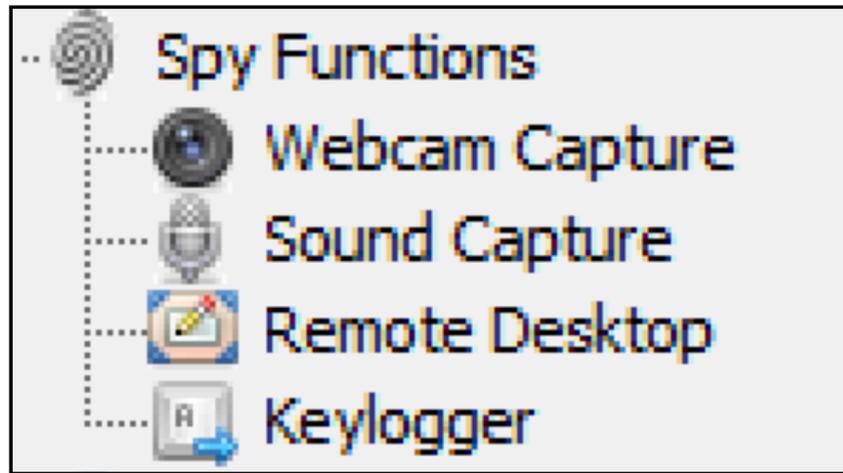
777  
sessions



# Remote Desktop

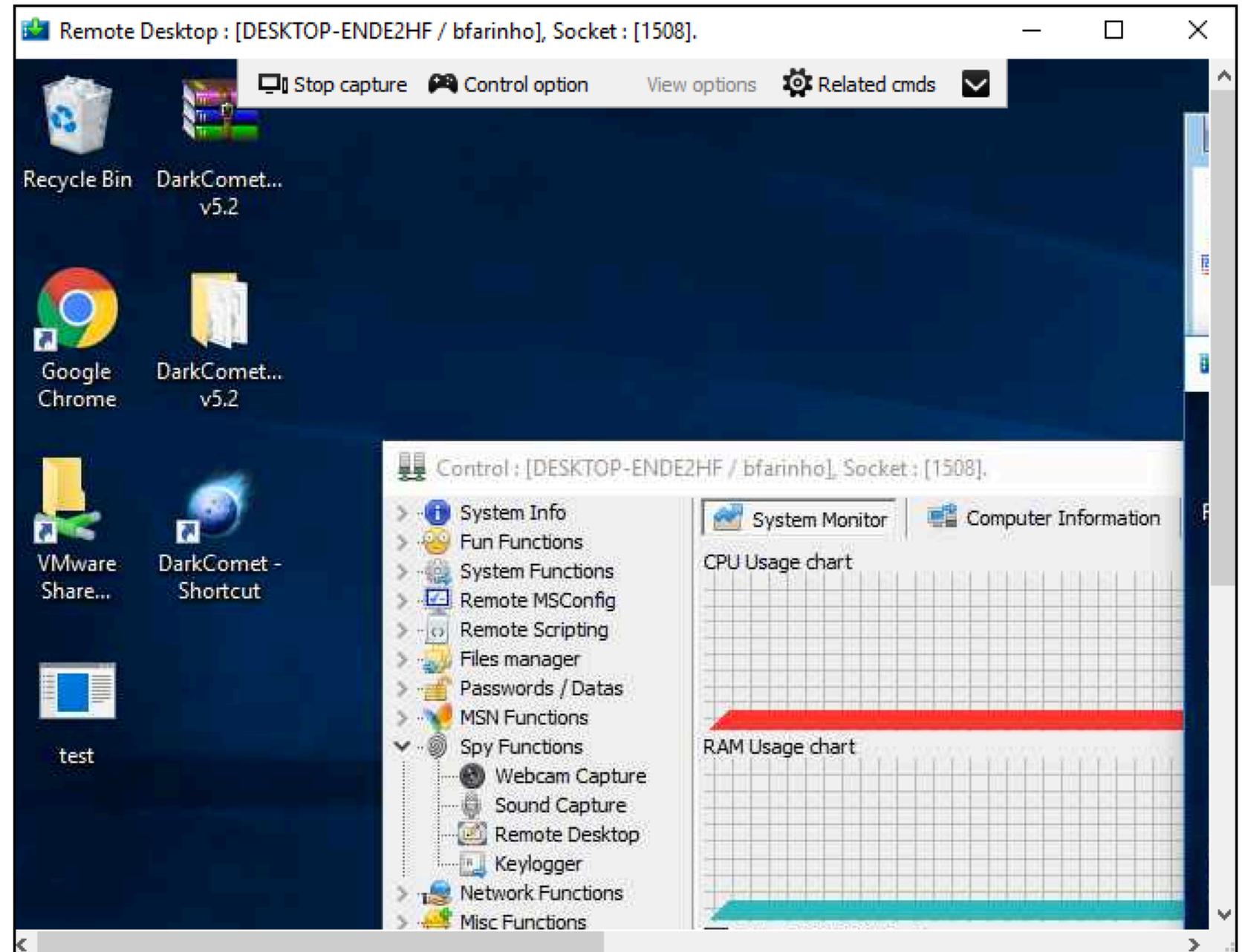
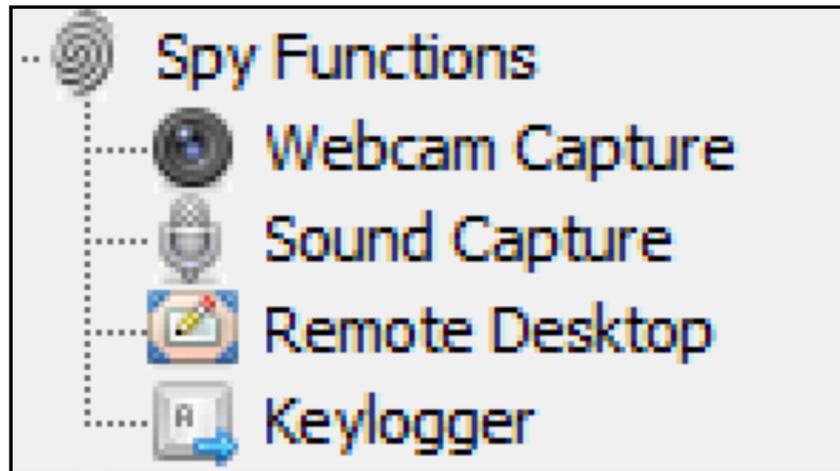


# Remote Desktop



Remote Desktop: **83%** !

# Remote Desktop

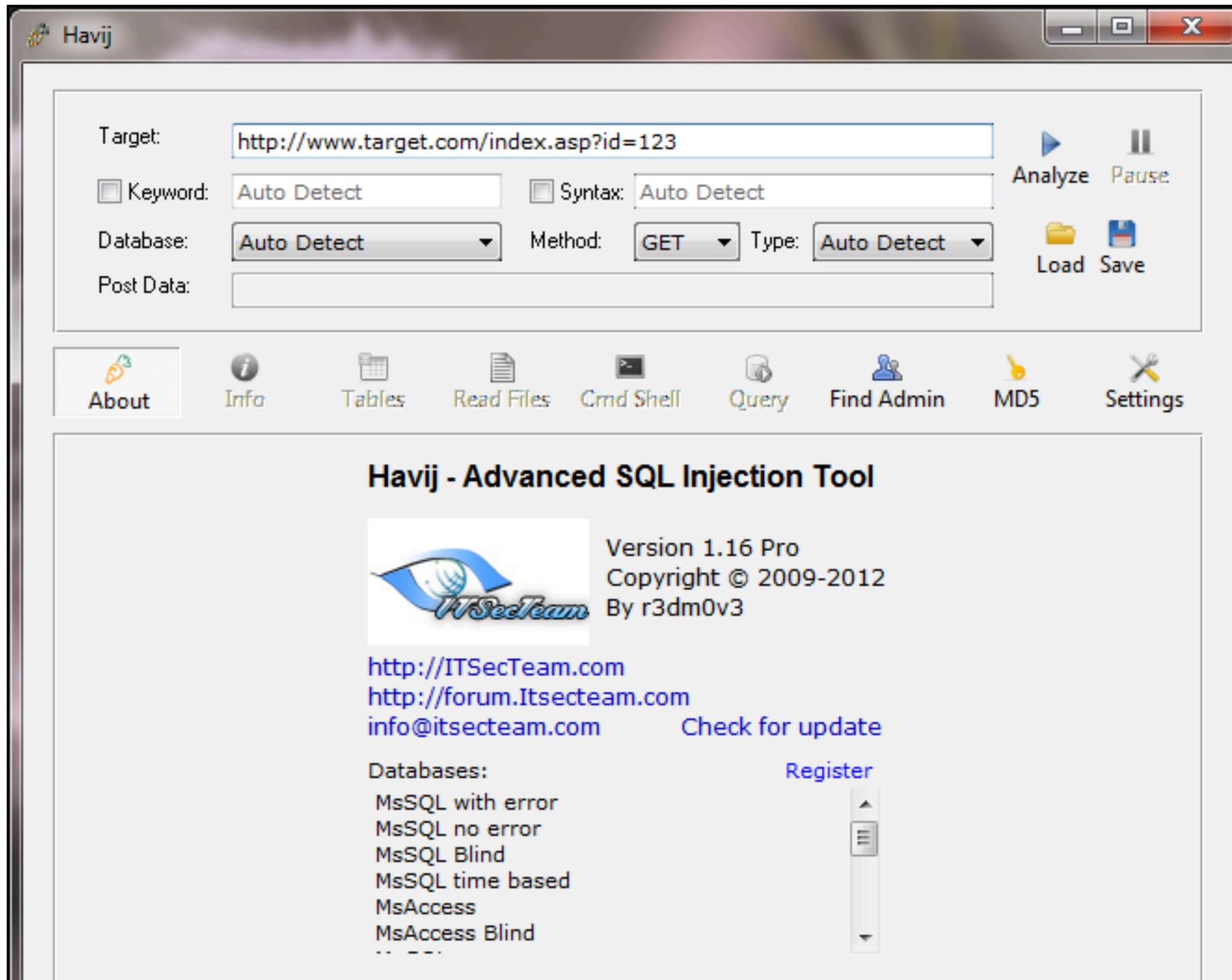


Remote Desktop: **83%** !

**Active** RD: **56%**

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

# Remote Desktop



## Havij SQL Injector

# Remote Desktop

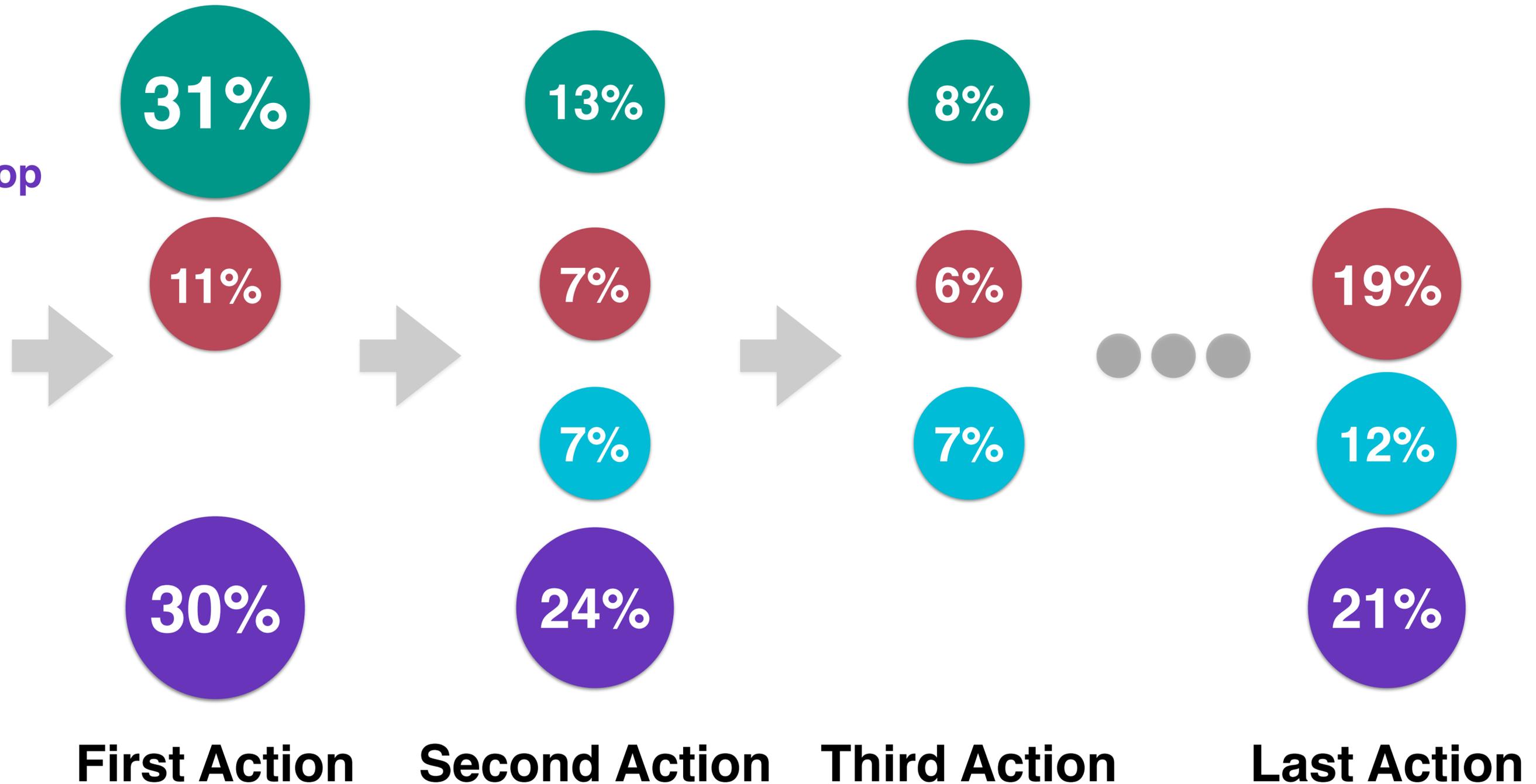
The screenshot shows a web browser window with the URL [http://s4.dosya.tc/server2/qcgw2i/3.0.11.2\\_TeamSpeak3\\_Windows.rar.html](http://s4.dosya.tc/server2/qcgw2i/3.0.11.2_TeamSpeak3_Windows.rar.html). The page is from the website **dosya.tc** and displays the file **3.0.11.2\_TeamSpeak3\_Windows.rar** for download. The file size is 3.56 MB and it has been downloaded 19 times. A large green button labeled **START DOWNLOAD** is prominent. Below it, there are instructions for unzipping the file, including a **GoUnzip** logo. A second **START DOWNLOAD** button is also visible. At the bottom of the browser window, a Windows file explorer dialog asks: "Do you want to open or save 3.0.11.2\_TeamSpeak3\_Windows.rar (3.56 MB) from s4.dosya.tc?". The taskbar at the bottom shows various application icons and the system clock indicates 9:30 AM on 10/27/2016.

**TeamSpeak 3  
(gaming server)**

# Common Patterns of Action

- Webcam, Audio
- Passwords
- Filesystem
- Remote Desktop

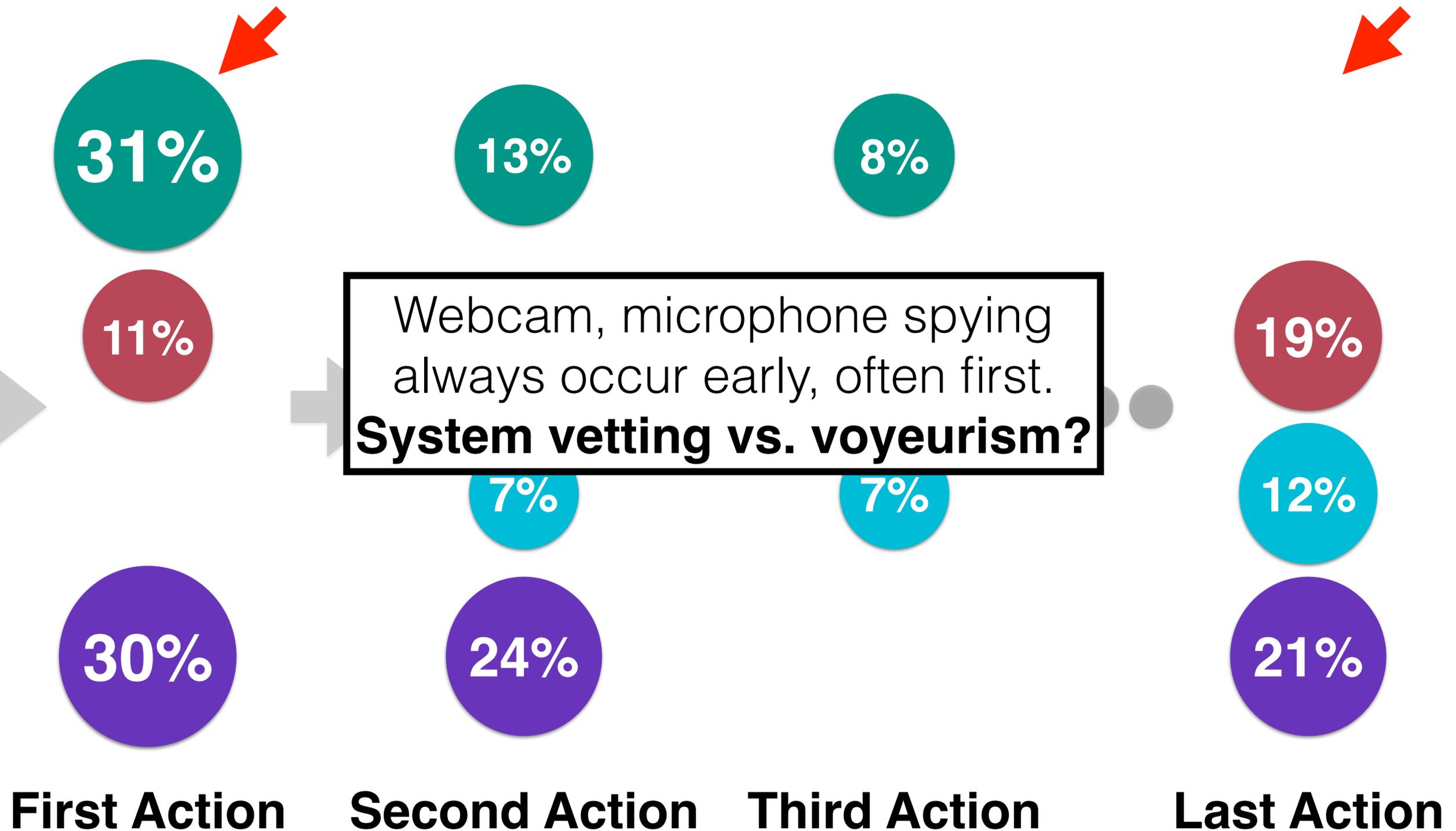
777  
sessions



# Common Patterns of Action

- Webcam, Audio
- Passwords
- Filesystem
- Remote Desktop

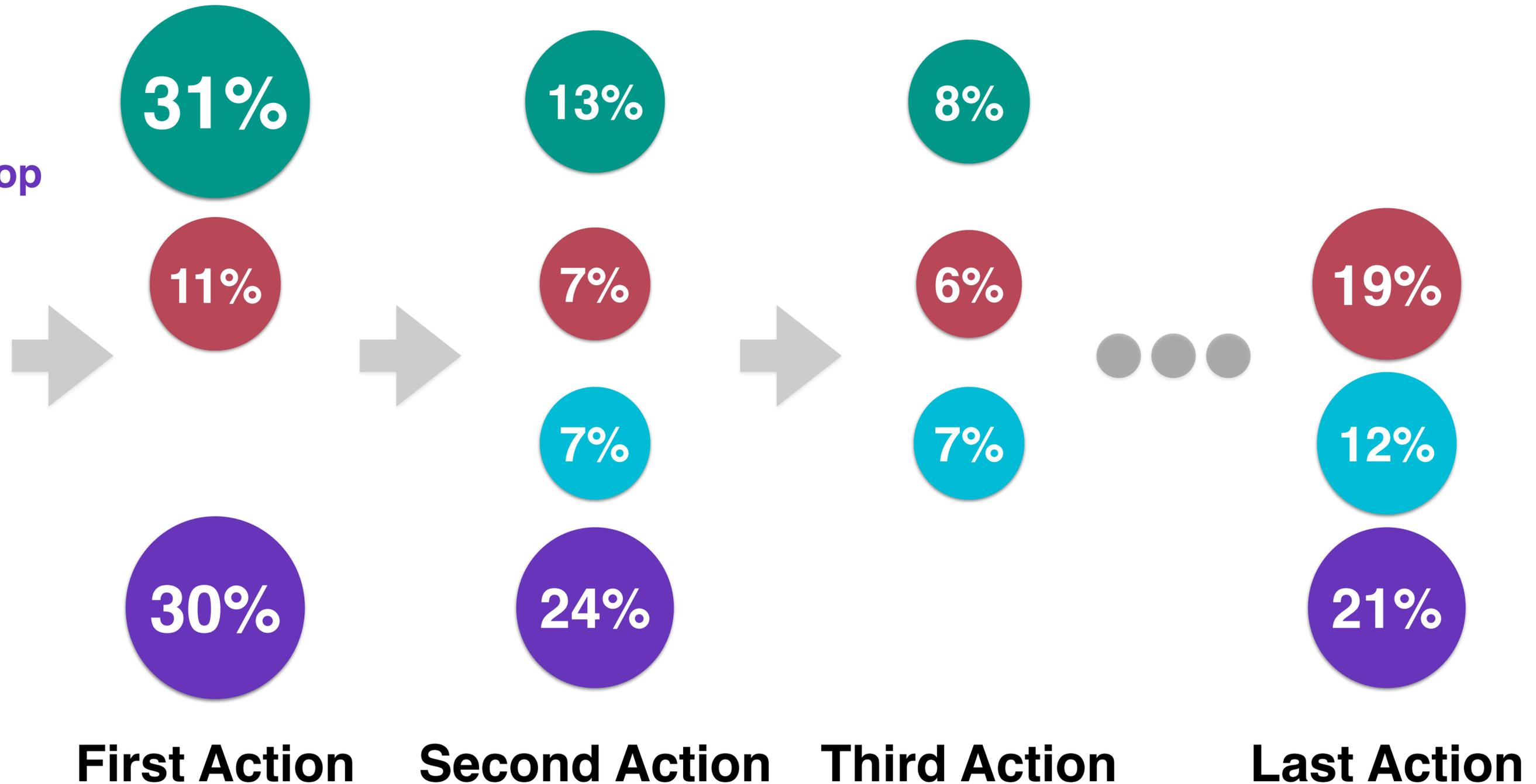
777  
sessions



# Common Patterns of Action

- Webcam, Audio
- Passwords
- Filesystem
- Remote Desktop

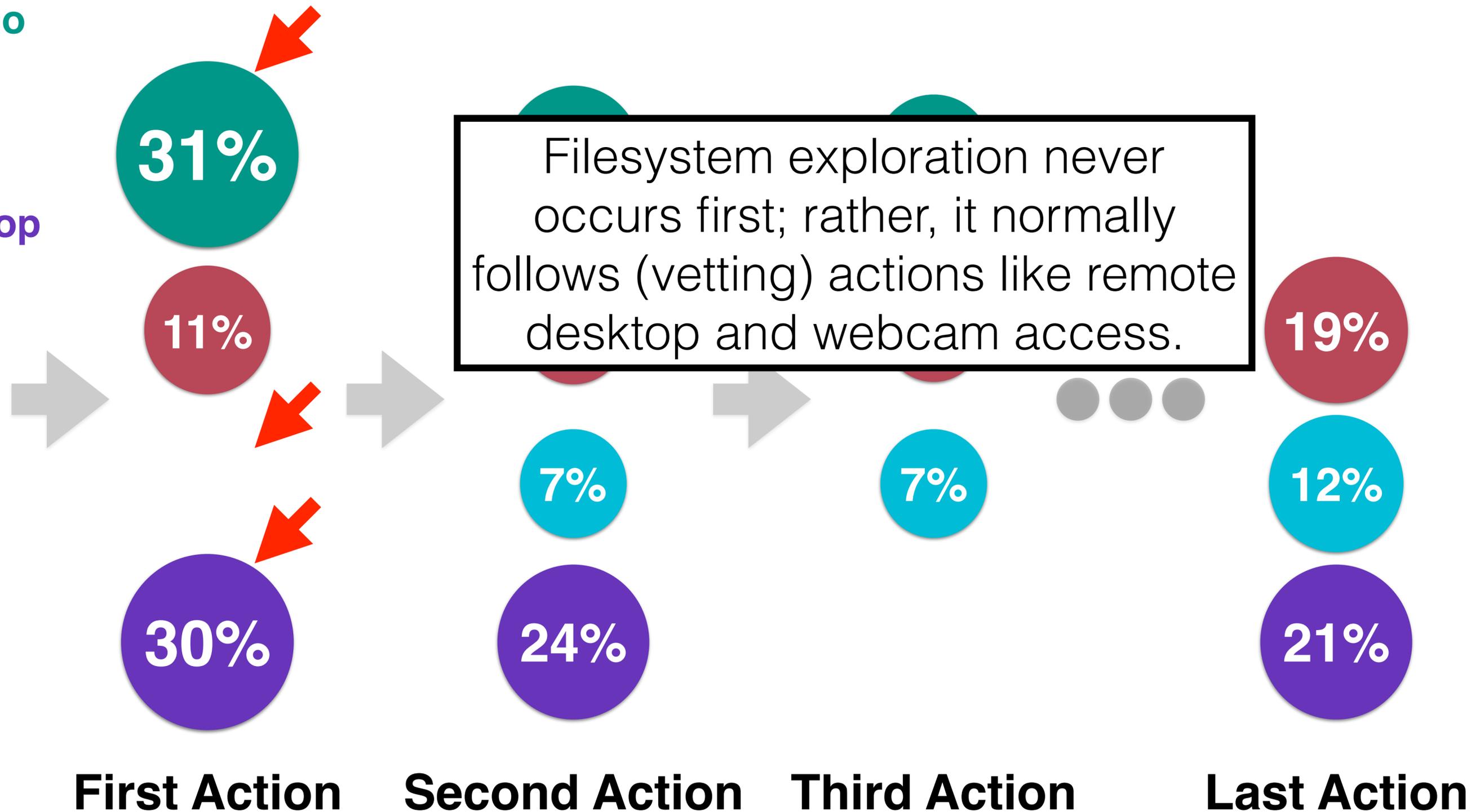
777  
sessions



# Common Patterns of Action

- Webcam, Audio
- Passwords
- Filesystem
- Remote Desktop

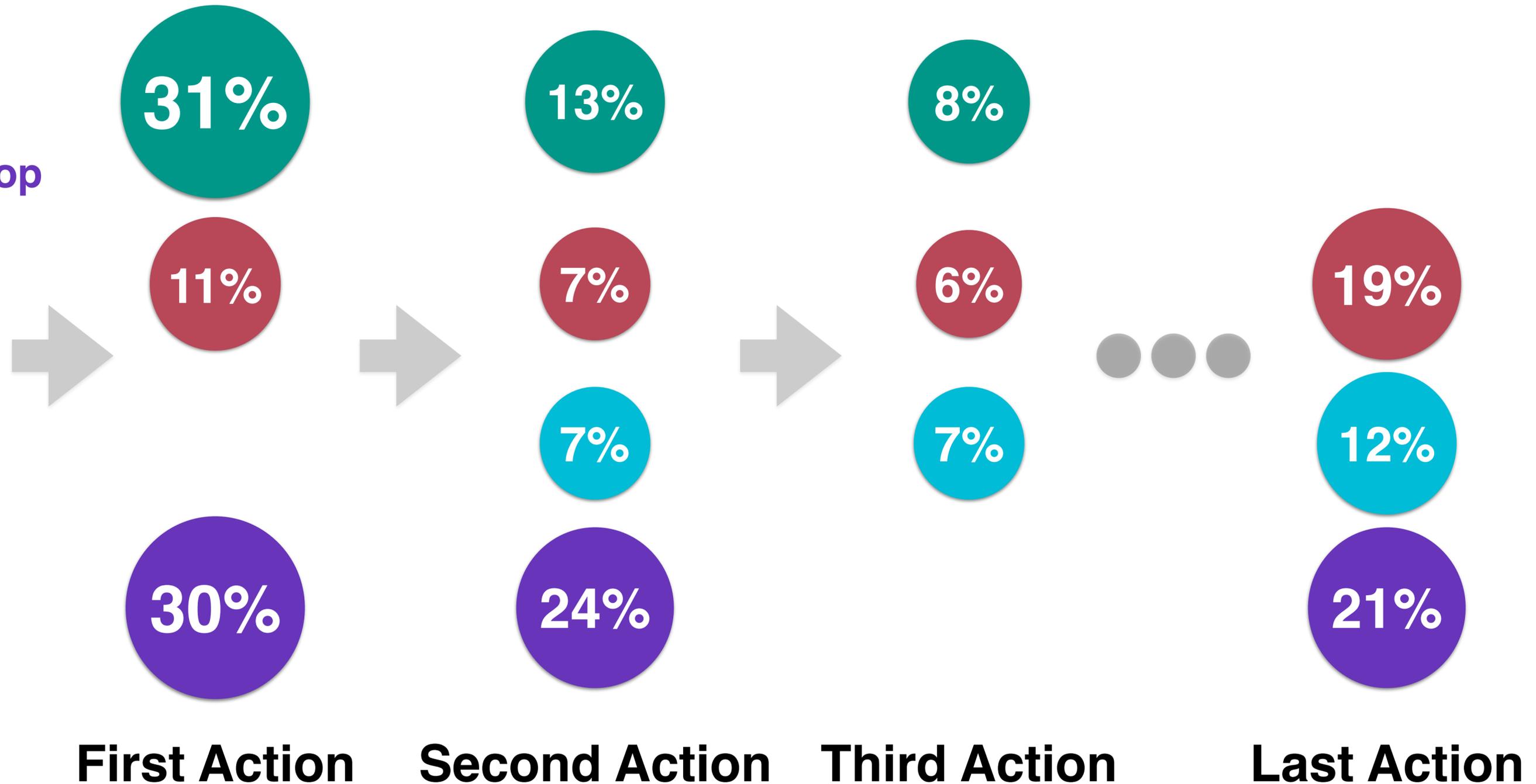
777  
sessions



# Common Patterns of Action

- Webcam, Audio
- Passwords
- Filesystem
- Remote Desktop

777  
sessions

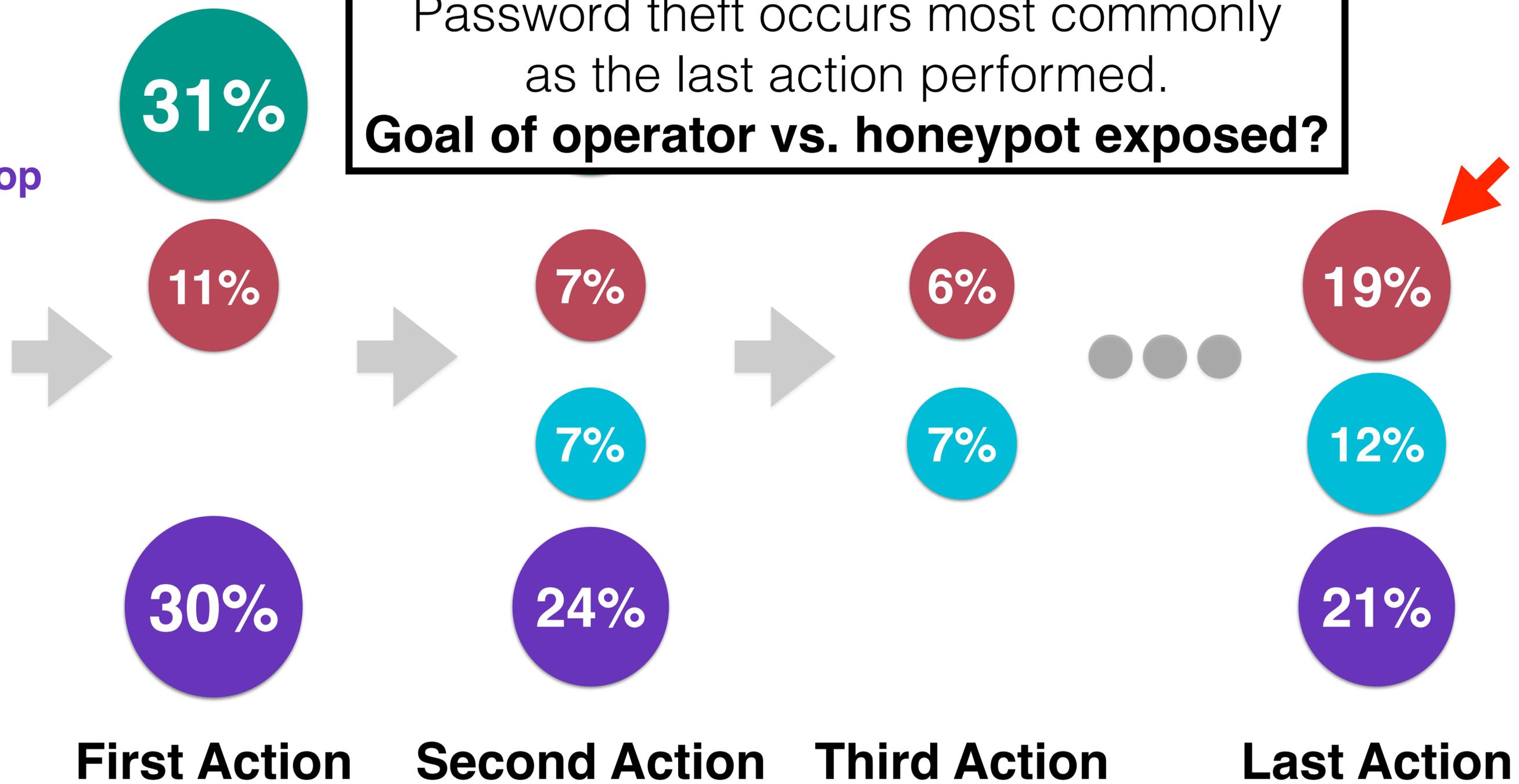


# Common Patterns of Action

- Webcam, Audio
- Passwords
- Filesystem
- Remote Desktop

Password theft occurs most commonly as the last action performed.  
**Goal of operator vs. honeypot exposed?**

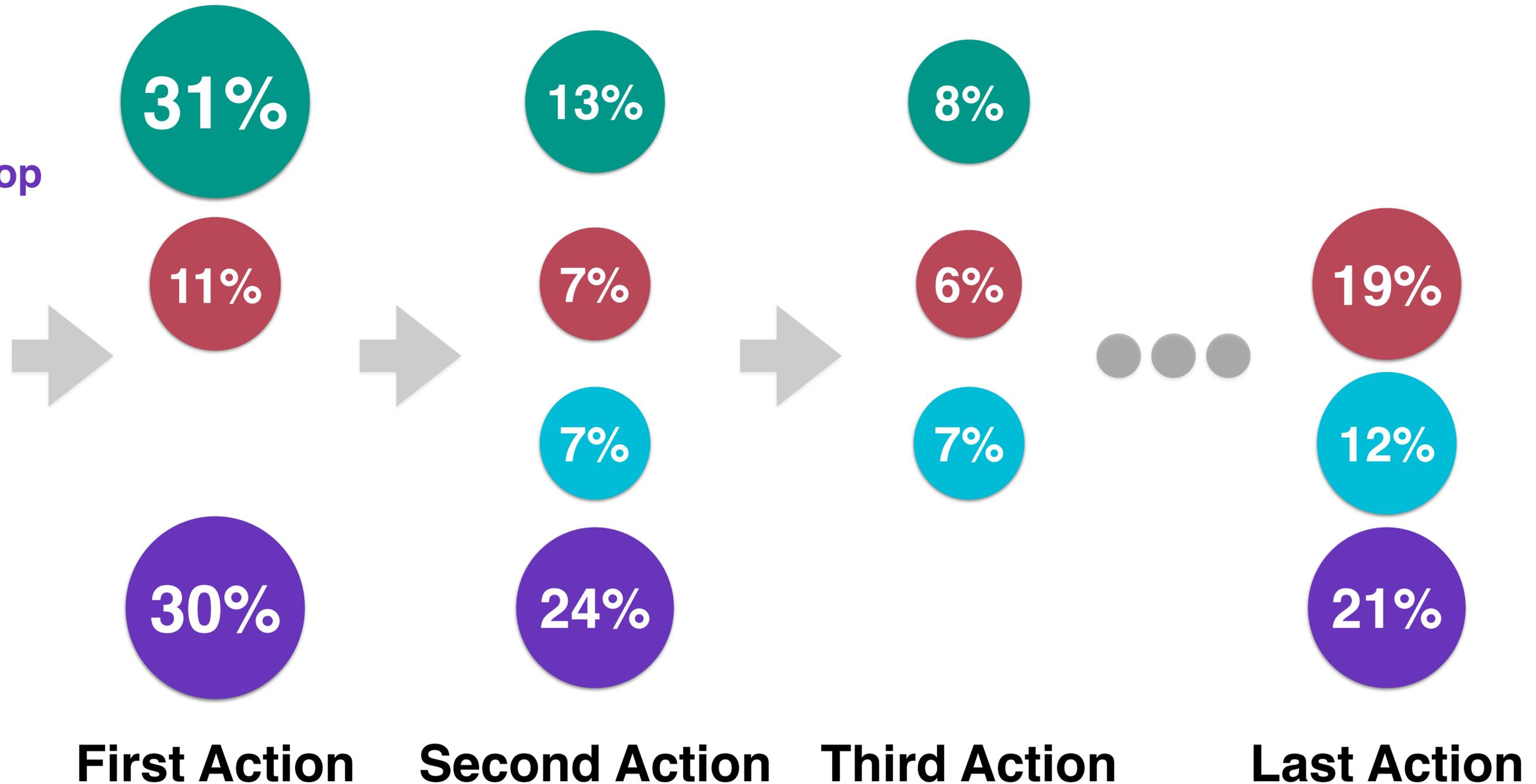
777 sessions



# Common Patterns of Action

- Webcam, Audio
- Passwords
- Filesystem
- Remote Desktop

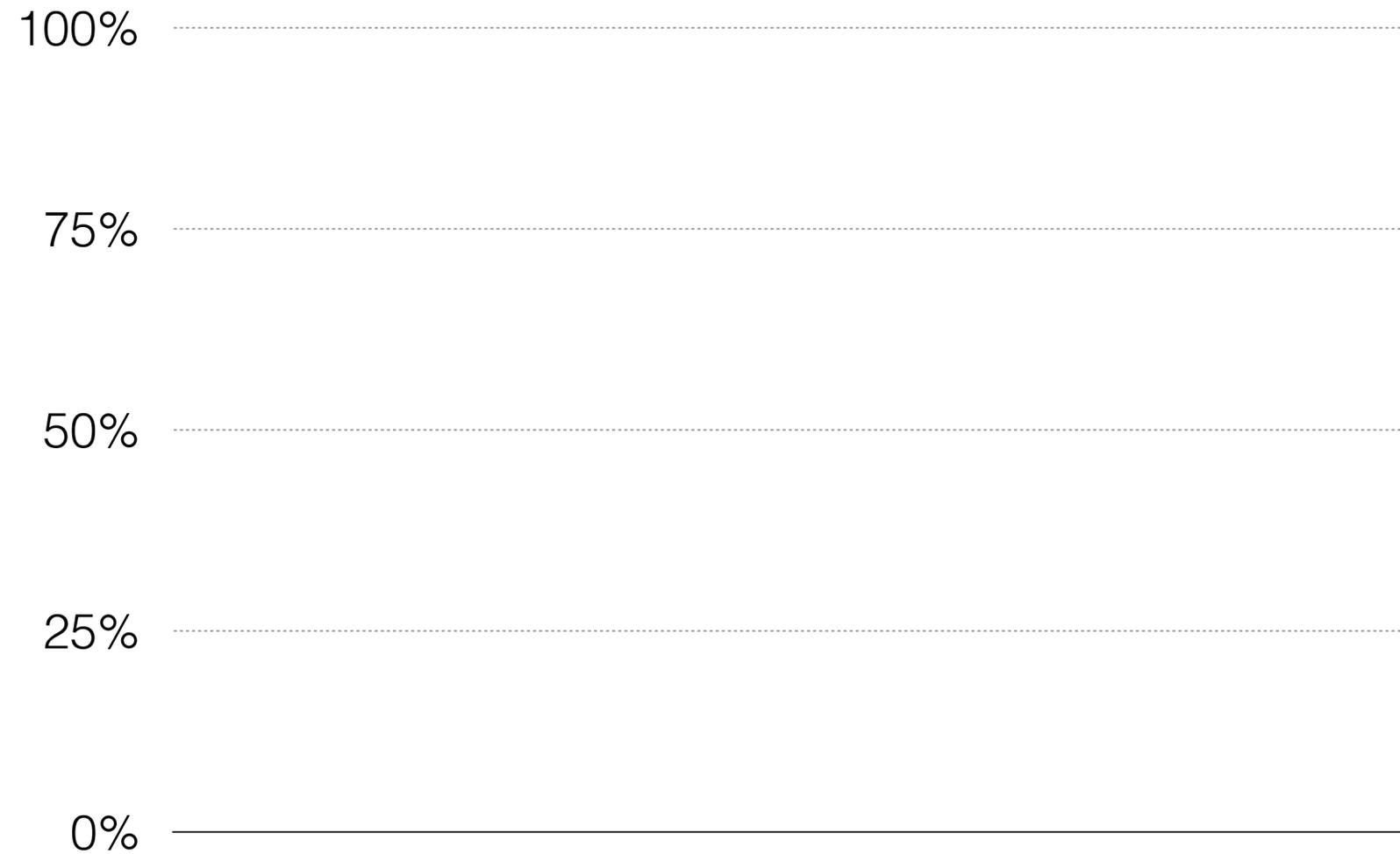
777  
sessions



# Overall Trends in Dataset



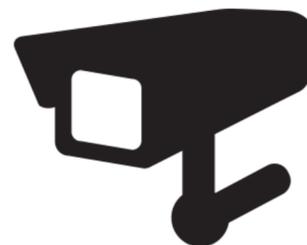
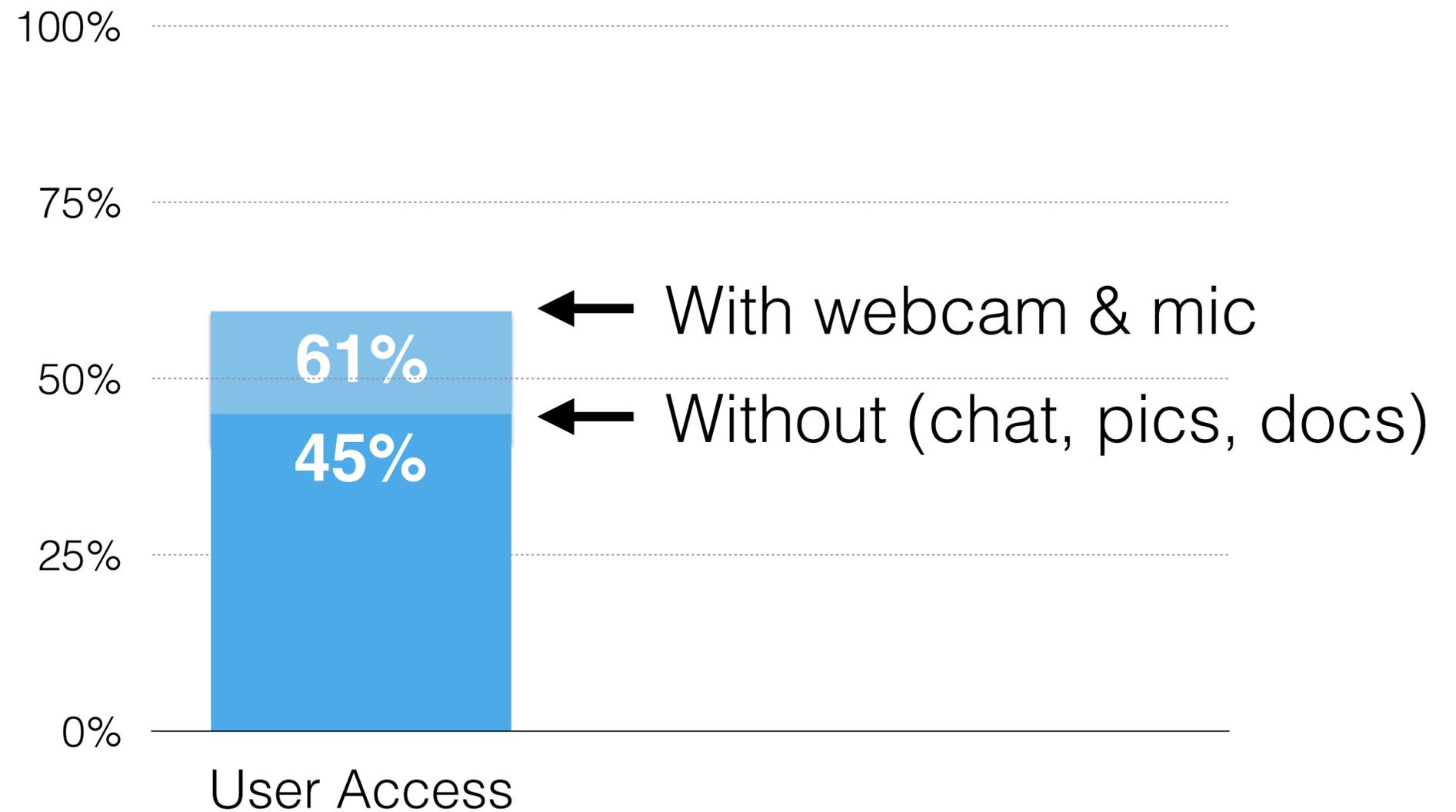
What **resource(s)** are RAT operators after?



# Overall Trends in Dataset



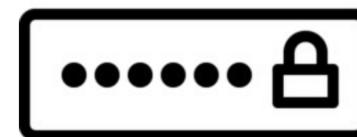
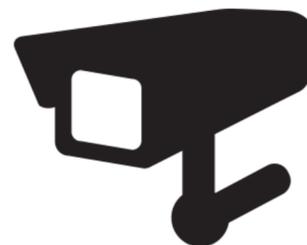
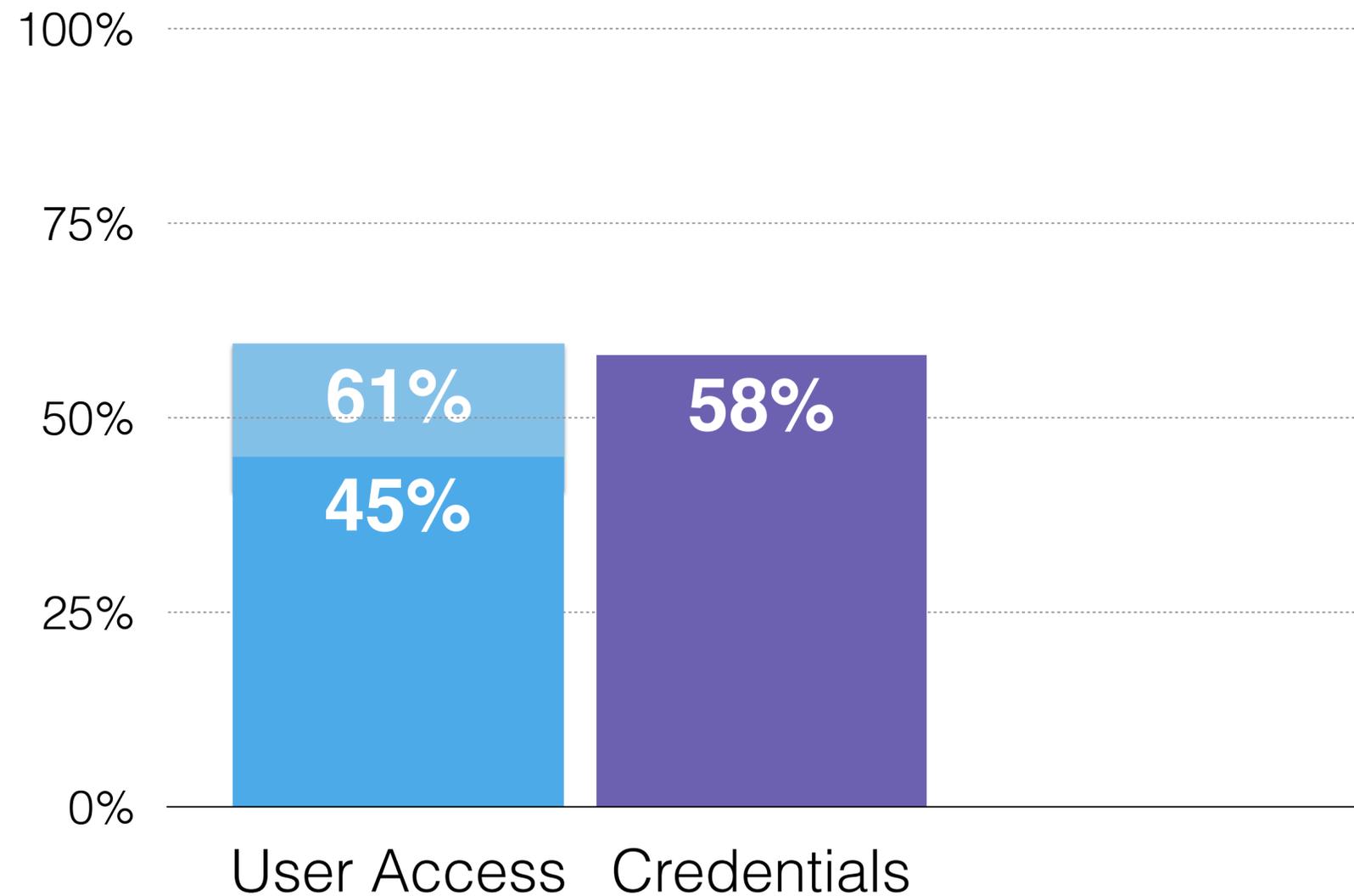
What **resource(s)** are RAT operators after?



# Overall Trends in Dataset



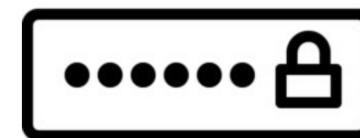
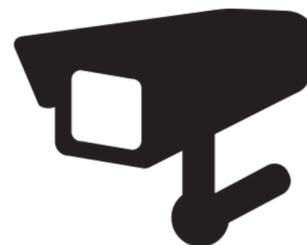
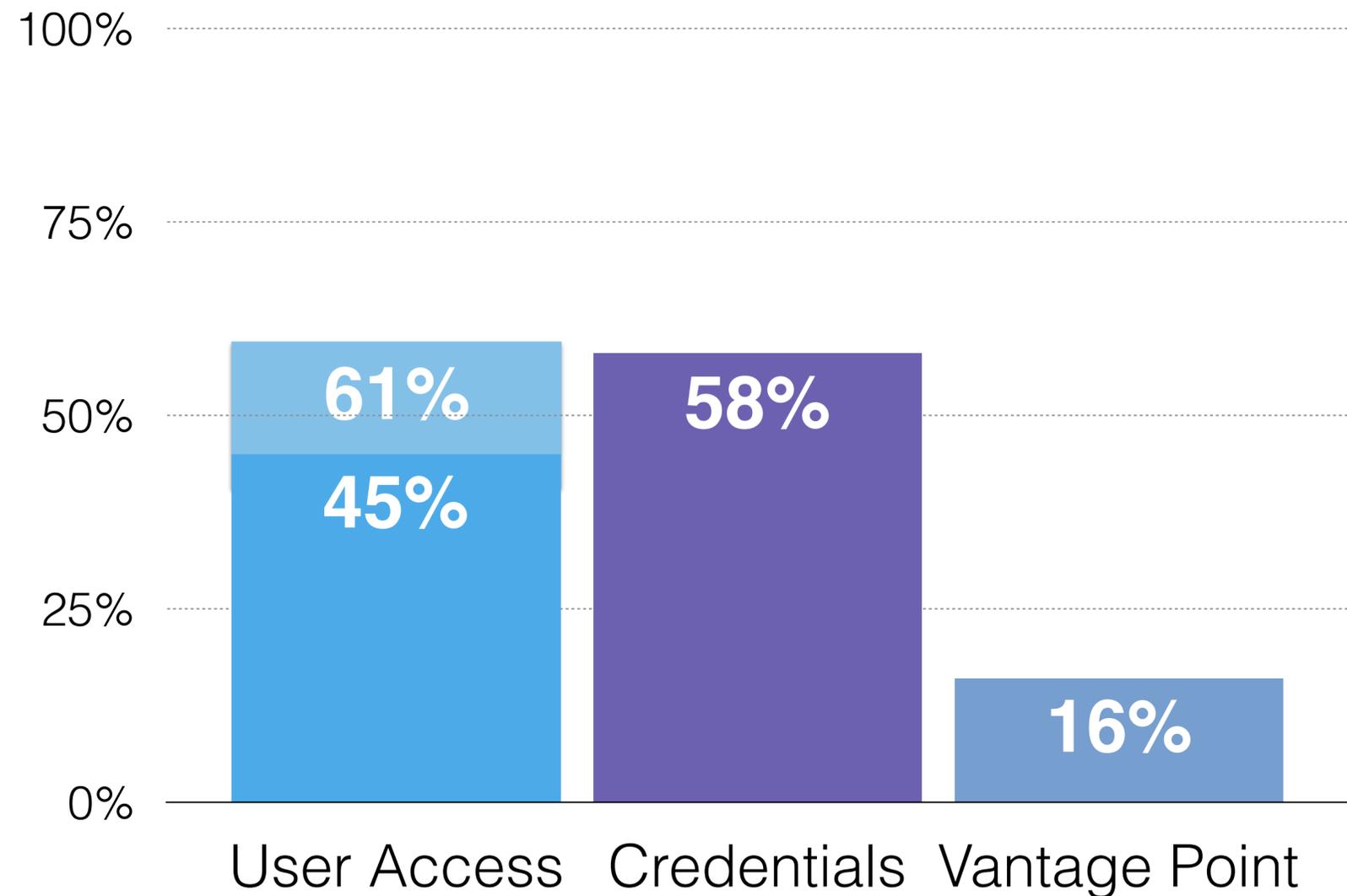
What **resource(s)** are RAT operators after?



# Overall Trends in Dataset



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

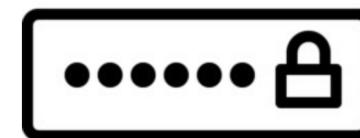
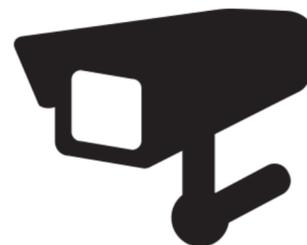
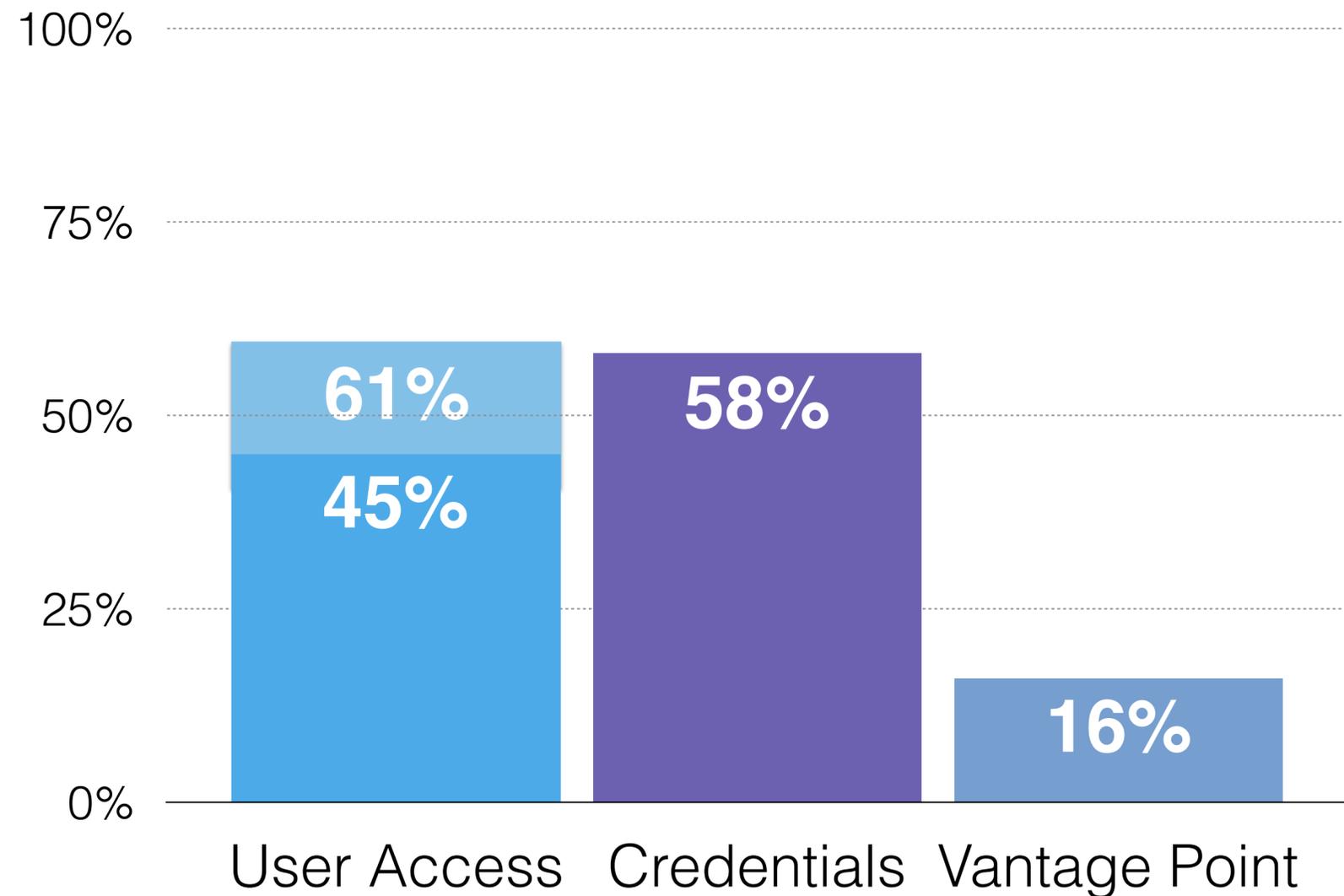


# Overall Trends in Dataset



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

- RATs are for user access

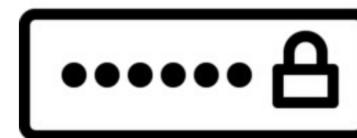
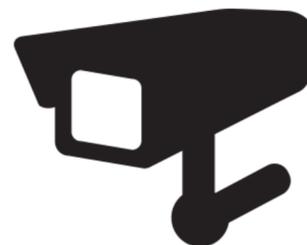
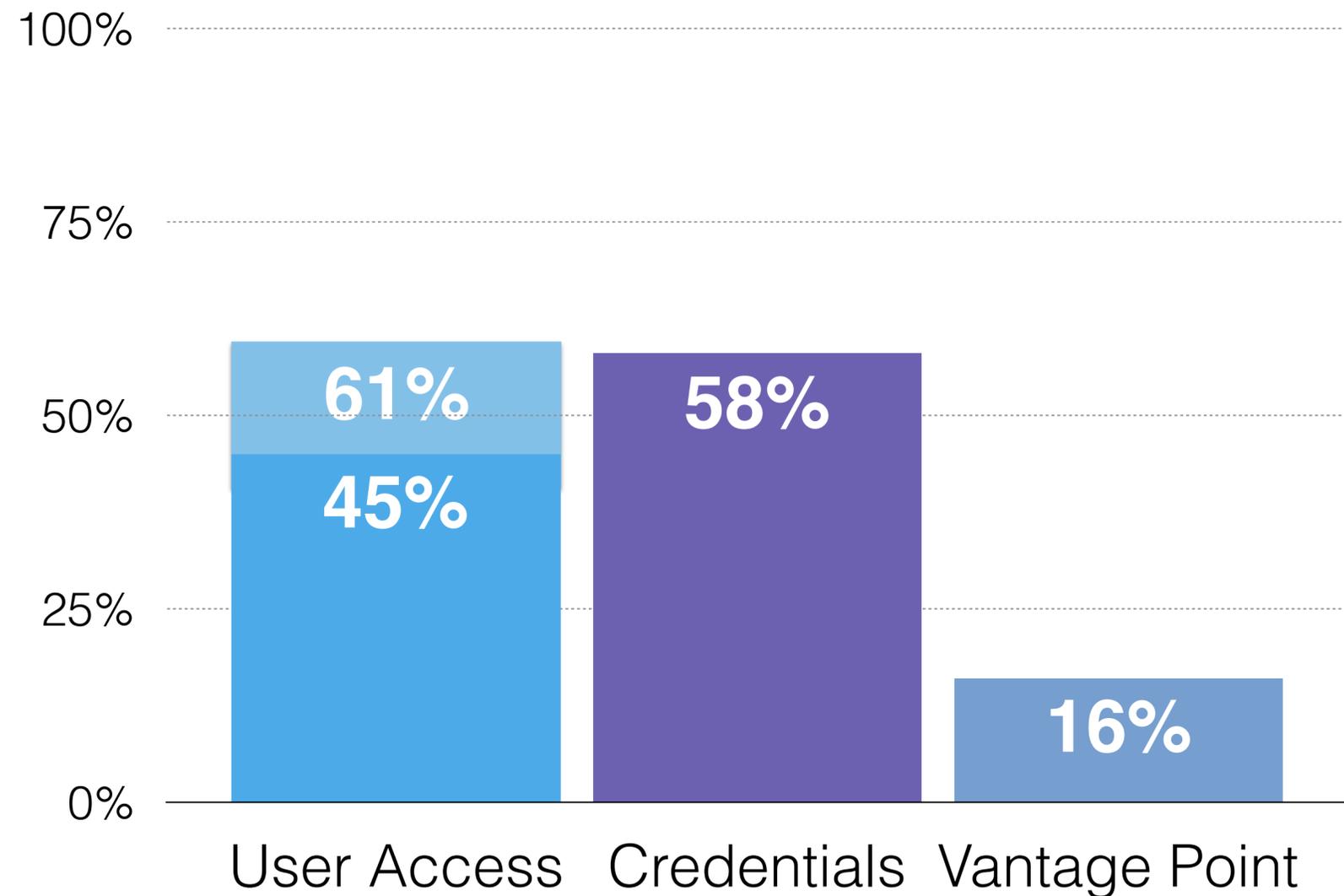


# Overall Trends in Dataset



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

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

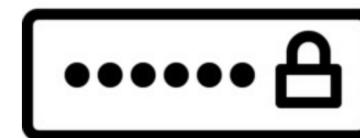
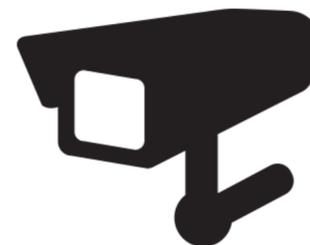
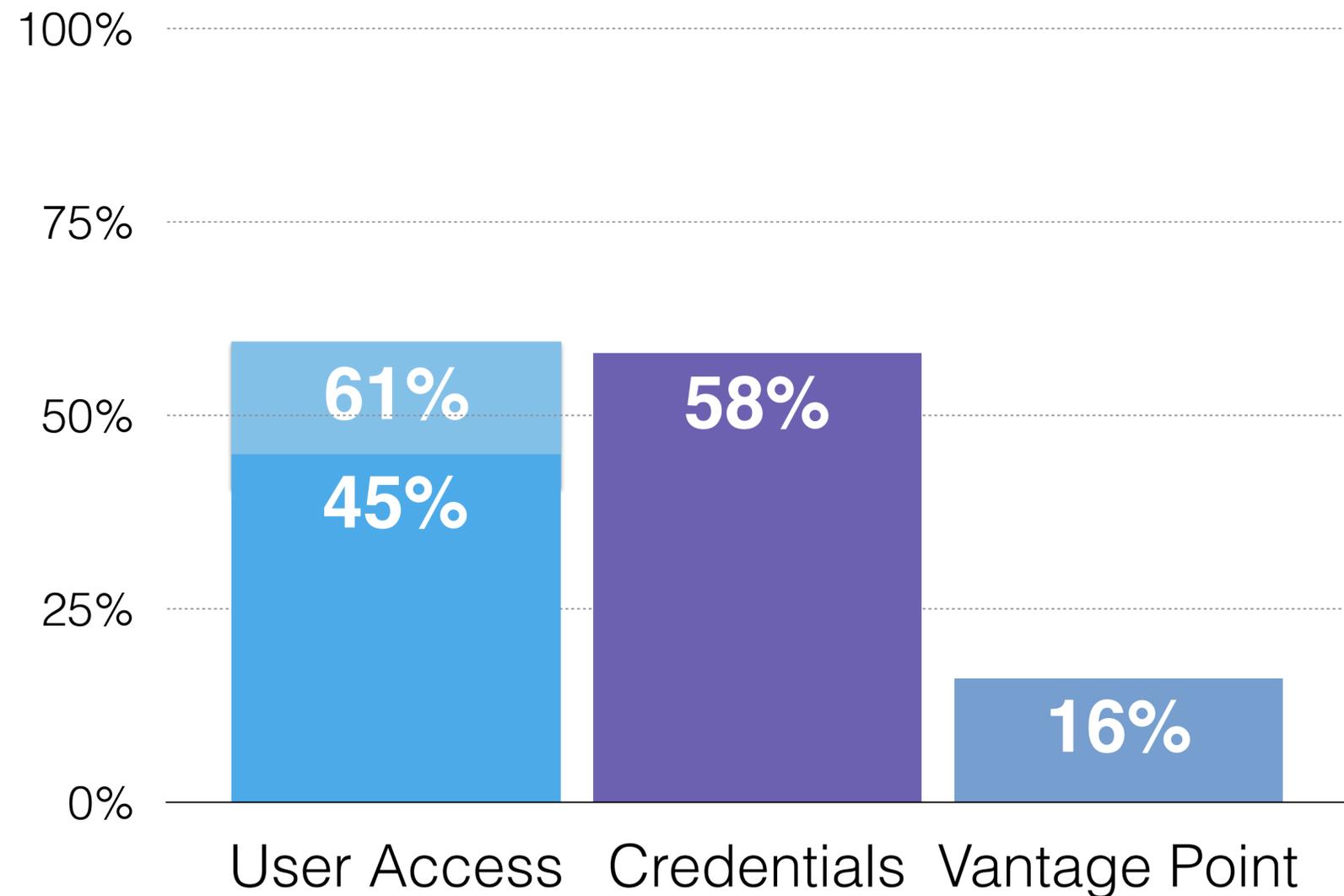


# Overall Trends in Dataset



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](mailto:bfarinho@cs.ucsd.edu)**



Backup Slides

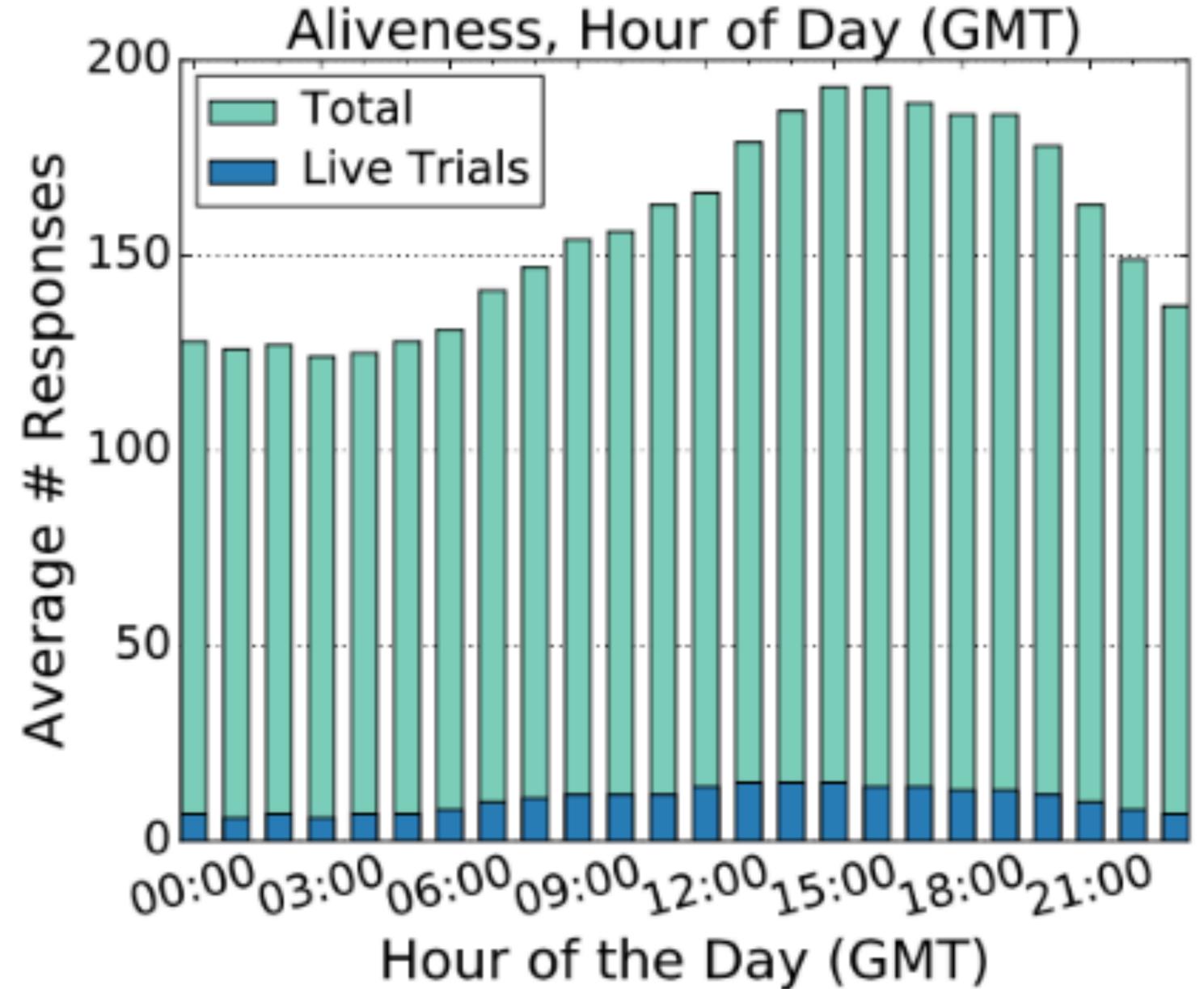
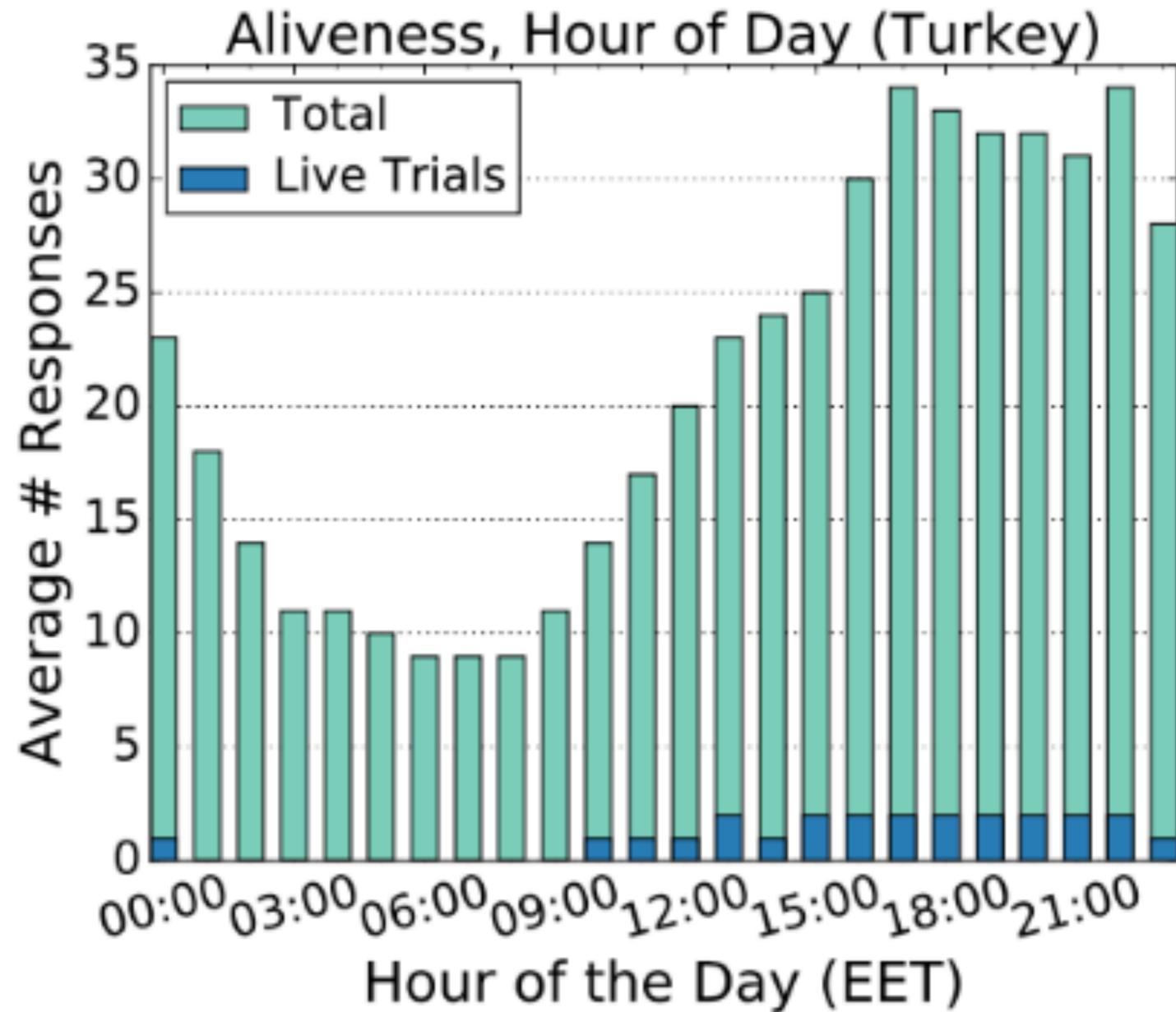
# Operator OpSec is Terrible

- 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

<b>Operator Country</b>	GB	•	•	•	1	•	•	•	2	5
	FR	•	•	•	•	•	•	•	11	•
	NL	•	•	•	1	•	•	2	2	•
	TH	•	•	•	1	•	13	•	6	•
	BR	•	•	•	2	15	•	•	3	•
	US	•	•	•	16	1	•	•	4	•
	UA	9	•	8	3	•	•	•	7	•
	TR	•	50	•	3	1	•	•	13	•
	RU	32	•	1	3	•	•	•	20	•
		RU	TR	UA	US	BR	TH	NL	FR	GB

**VT Uploader 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**

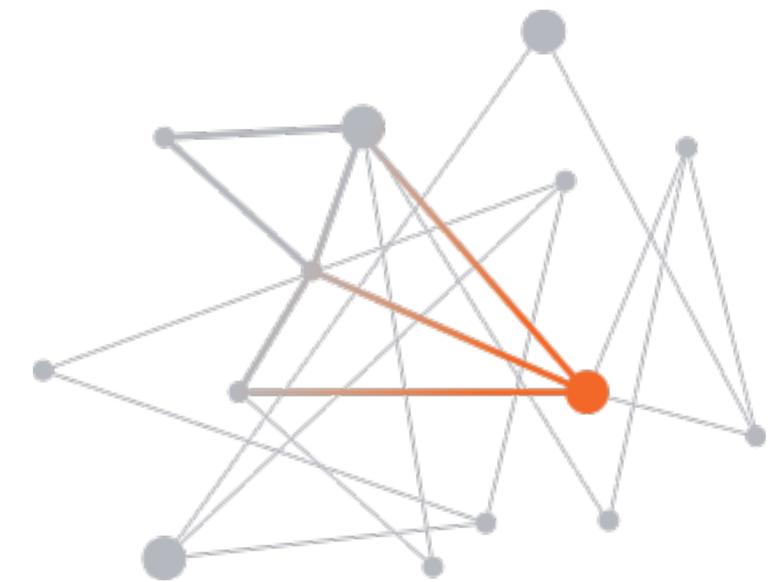


# Threat Intelligence

**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**