

ECE 498KL: eCrime and Internet Service Abuse

Remote Access Trojans

Kirill Levchenko

December 11, 2018

I ILLINOIS

Electrical & Computer Engineering

COLLEGE OF ENGINEERING

Remote Access Trojans

- ❖ Let attackers interactively control infected machine
- ❖ Access to webcam and microphone
- ❖ Browse file system, steal files, passwords, cookies
- ❖ Install additional malware
- ❖ Interact with victim via chat and alerts
- ❖ Remote desktop capability
- ❖ Extract more value from target
- ❖ High operator overhead (per infection)

Low Barrier to Entry

Availability:
YouTube

Community: Dedicated
Hacking Forums

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 of download dark comet here: <http://ge.tu5jnRAPF2/v/0> ...

How to Download and Use DarkComet 5.3.1 - YouTube



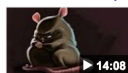
<https://www.youtube.com/watch?v=VdbFYAVKoDw>
Mar 12, 2013 - Uploaded by N3rdizzle
LINKS: DarkComet 5.3.1: <http://www.mediafire.com/?emhkqegn7774i4o>
Sandboxie: <http://www.sandboxie.com> ...

How to Download and Use DarkComet 5.3.1 (2016 updated) - YouTube



<https://www.youtube.com/watch?v=58kSMFoNys>
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 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/#!e1BC3LQB!>

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 ...

Hack Forums Packets, Punks, and Posts

Home Upgrade Search Members Extras Wiki Help Follow Contact

Welcome back, [User Name]
View New Posts | Your Threads | Your Posts | Private Messages (Unread 0, Total 1) Open Buddy List

Hack Forums / Search / Results

Pages (25): 1 2 3 4 5 ... 25 Next >

Search Results	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)	MySErIoUs-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: TheTwoSeerflooms
[DarkComet] RATi [DarkComet] (Outdated) (1 2)	Marijuana x	Hacking Tutorials	19	06-22-2016 12:02 PM Last Post: Stack
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

RAT Usage

Voyeurism

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

Sextortion & Blackmail

- SoCal RAT sextortionist
- Miss Teen USA

Surveillance & Espionage

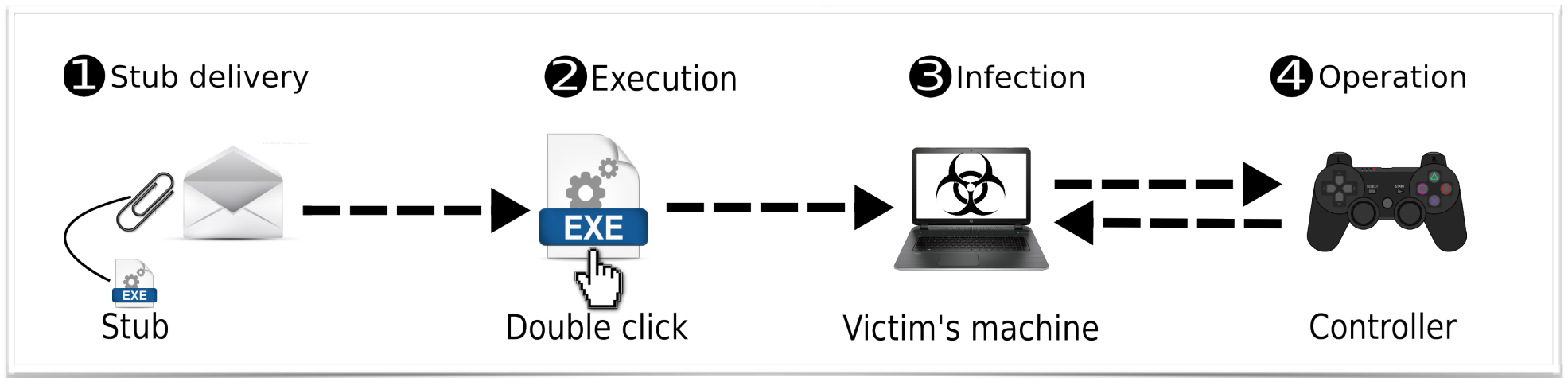
- Syria DarkComet Skype tool

**Common Theme:
*Access to Victim User***

RAT Vocabulary

- ❖ **Stub:** malware running on victim machine
- ❖ **Builder:** software to create and configure stubs
- ❖ **Controller:** Software used by operator to control stubs
- ❖ Controller and builder may be integrated

RAT Process



- ❖ **Stub initiates connection to controller**
 - Usually controller (command-and-control) domain part of stub
- ❖ **Controller then issues interactive commands to stub**

Research Questions



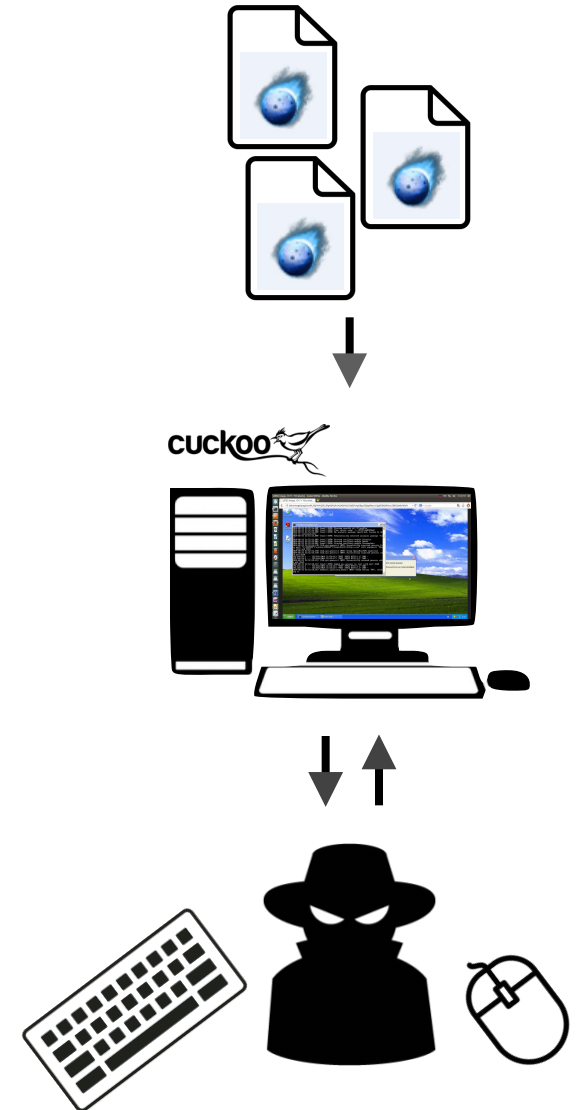
What do RAT operators do with compromised machines?

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

- RATs facilitate criminal behavior
- Understand the threat landscape
- Inform defenses

Methodology

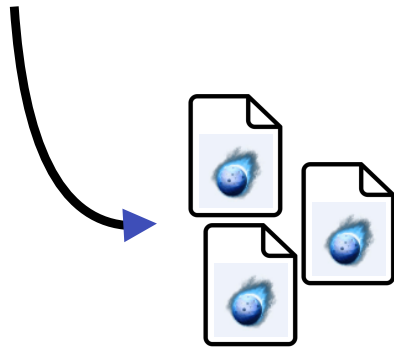
- ❖ Acquired DarkComet RAT samples
 - Samples are RAT *stubs*
- ❖ Executed them in malware sandbox honeypots
- ❖ Recorded network traces of operator interaction
- ❖ Decrypted to obtain operator command sequences



Sample Collection

 **virus**total

19,109
samples

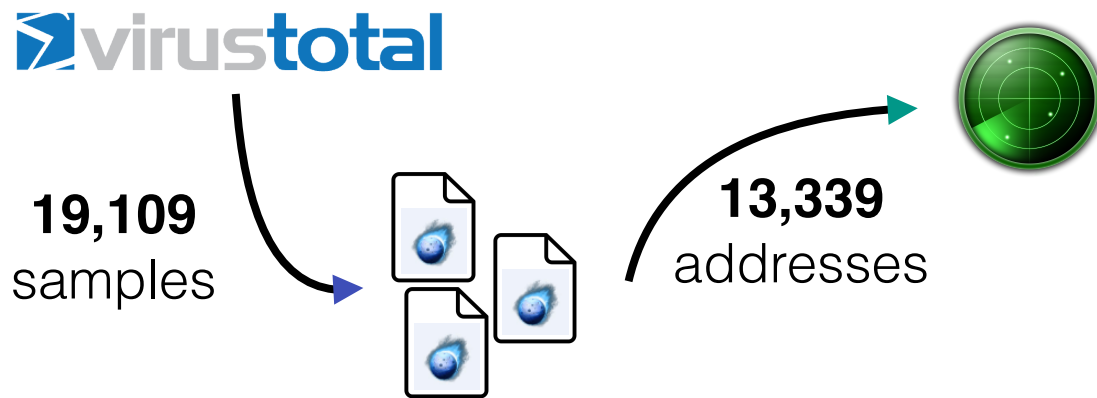


- ❖ *How are samples collected?*
- ❖ VirusTotal malware repository
 - Users can upload file for analysis by major AV vendors
 - Sometimes used as a free AV
 - Provides samples to “security community”

Sample Language Features

<i>Source</i>	<u><i>Domain Names</i></u>		<u><i>Campaign IDs</i></u>		<u><i>Filenames</i></u>	
	<i>Cnt</i>	<i>Pct</i>	<i>Cnt</i>	<i>Pct</i>	<i>Cnt</i>	<i>Pct</i>
English	321	24%	236	48%	381	38%
Turkish	56	4%	32	6%	38	3%
German	49	3%	3	-	6	-
Spanish	22	1%	7	1%	9	-
Vietnamese	18	1%	5	1%	12	1%
<i>Other</i>	269	20%	93	19%	131	13%
<i>Undetermined</i>	555	43%	110	22%	401	41%
<i>Total</i>	1,290		486		978	

Extracting C&C Domains



- ❖ *How are command-and-control domains extracted?*
- ❖ RAT stub configuration contains password, campaign name, and controller command-and-control domains

Extracting C&C Domains

 **virustotal**

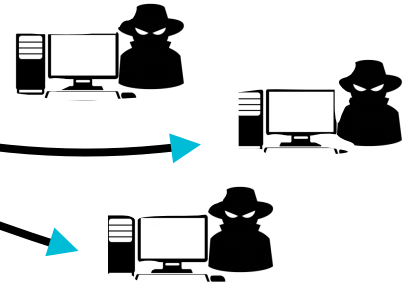
19,109
samples



13,339
addresses

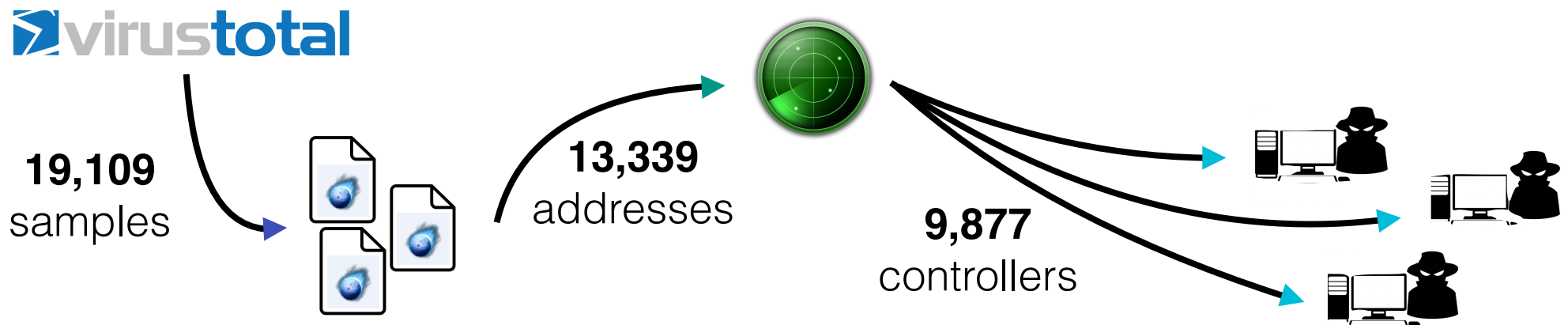


9,877
controllers



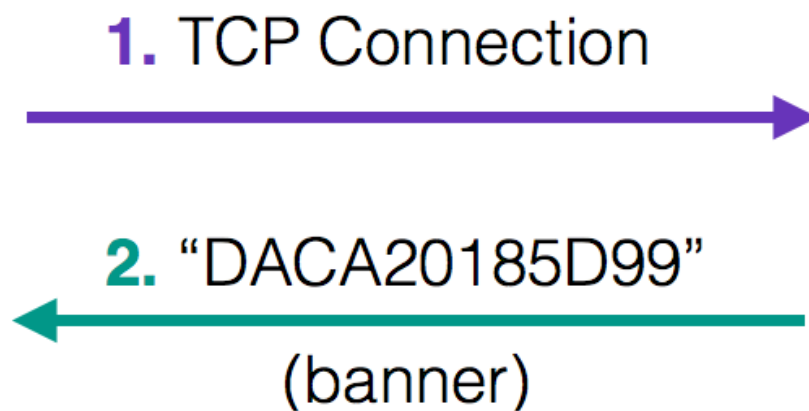
- ❖ *How are the controllers monitored?*
- ❖ Resolve C&C domain, then initiate protocol connection

Extracting C&C Domains



- ❖ *Why are the controllers monitored?*
- ❖ Only run stub in VM if controller is online
 - Can't run all stubs at once — limited researcher resources

DarkComet Communication Protocol

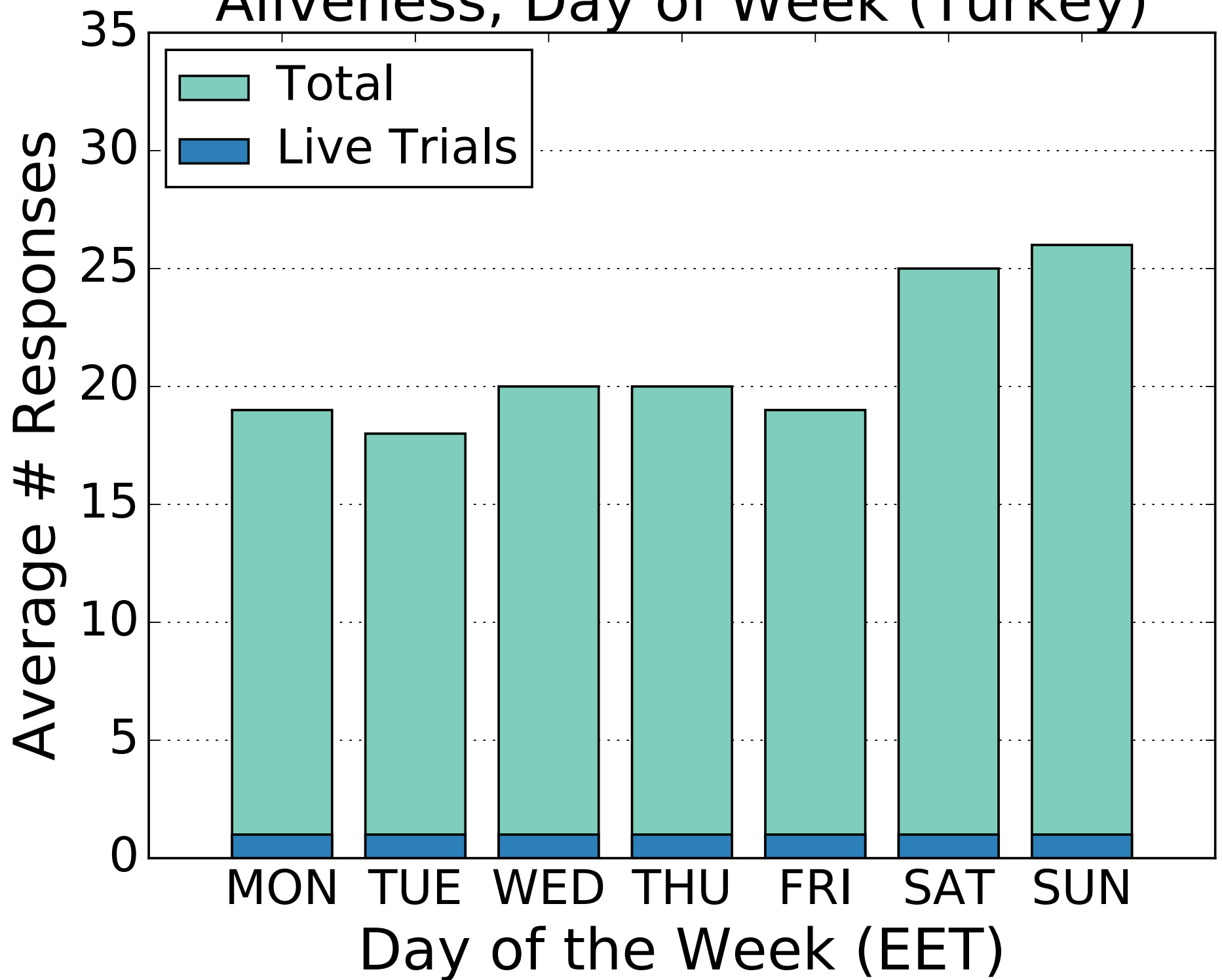


== "IDTYPE" **RC4-encrypted**
(key in sample), hex-encoded

Controller IP Location

<i>Country</i>	<i>Global Scanning</i>		<i>Live Trials</i>	
	<i>Cnt</i>	<i>Pct</i>	<i>Cnt</i>	<i>Pct</i>
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%
<i>Other</i>	3,512	36%	307	35%
<i>Total</i>	9,877		867	

Aliveness, Day of Week (Turkey)



Attacker–Victim Geography

- ❖ Have operator (attacker) IP address from monitoring
- ❖ VirusTotal includes uploader IP address
- ❖ Get location of IP addresses using geolocation services
 - Location information is imperfect
- ❖ **Note:** Operator may be using VPN or proxy
 - Location will be location of proxy or VPN endpoint

Controller Country	RU	TR	UA	US	BR	TH	NL	FR	GB	DE	GE	PK	RO	AU	IT	BY	KZ	AZ	CA	MD
MD	1	2	1	1
CA	5	.
AZ	.	.	.	1	.	.	.	2	1	.	.
KZ	.	.	.	1	.	.	.	1	1	.	2	.
BY	1	.	2	3
IT	2	3	.	.	.	2	.
AU	.	.	.	1	6
RO	1	.	.	1	.	.	.	2	3	.	.	1	.	.	1	.
PK	2	.	.	.	6	1	.
GE	2	.	.	5	2	.
DE	.	.	.	1	.	.	.	1	.	5	1	.
GB	.	.	.	1	.	.	.	2	5	3	.
FR	11	1	.
NL	.	.	.	1	.	.	2	2	.	1	8	.
TH	.	.	.	1	.	13	.	6	1	.
BR	.	.	.	2	15	.	.	3	3	.
US	.	.	.	16	1	.	.	4	7	.
UA	9	.	8	3	.	.	.	7	.	9	2	.
TR	.	50	.	3	1	.	.	13	9	.
RU	32	.	1	3	.	.	.	20	.	13	1	.	.	11	.

Uploader Country

Executing Samples

 virustotal

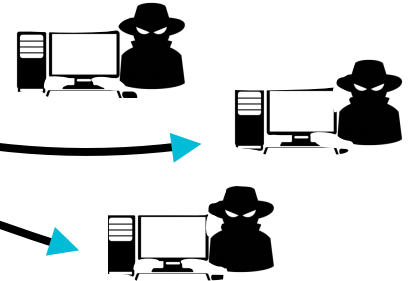
19,109
samples



13,339
addresses



9,877
controllers



1,165
live samples

cuckoo 



Honeypot Setup



- Installed Applications
- Populated Filesystem
 - *Documents, Pictures, Desktop*
- Browser History
- Credentials to Honey-Accounts

Honeypot Realism

- ❖ *Why does the honeypot need to look like a real PC?*
- ❖ Elicit natural attacker behavior

Operator Interactions



19,109
samples



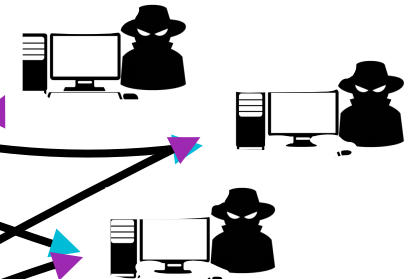
13,339
addresses



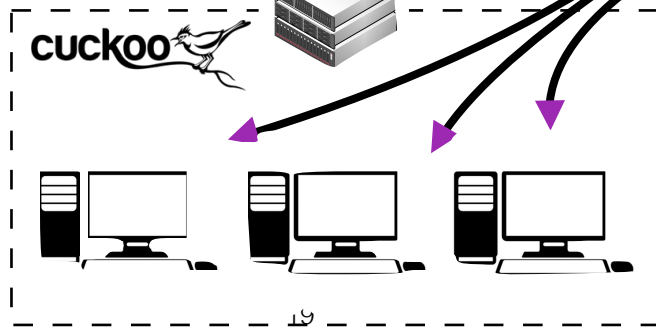
1,165
live samples



9,877
controllers



cuckoo



777
interactions



4 Weeks

Limitations

❖ *What are the limitations of this methodology?*

Targeted Attacks

We do *not* emulate specific targets.

DarkComet

DarkComet is a favorite of script kiddies.

Infection Longevity

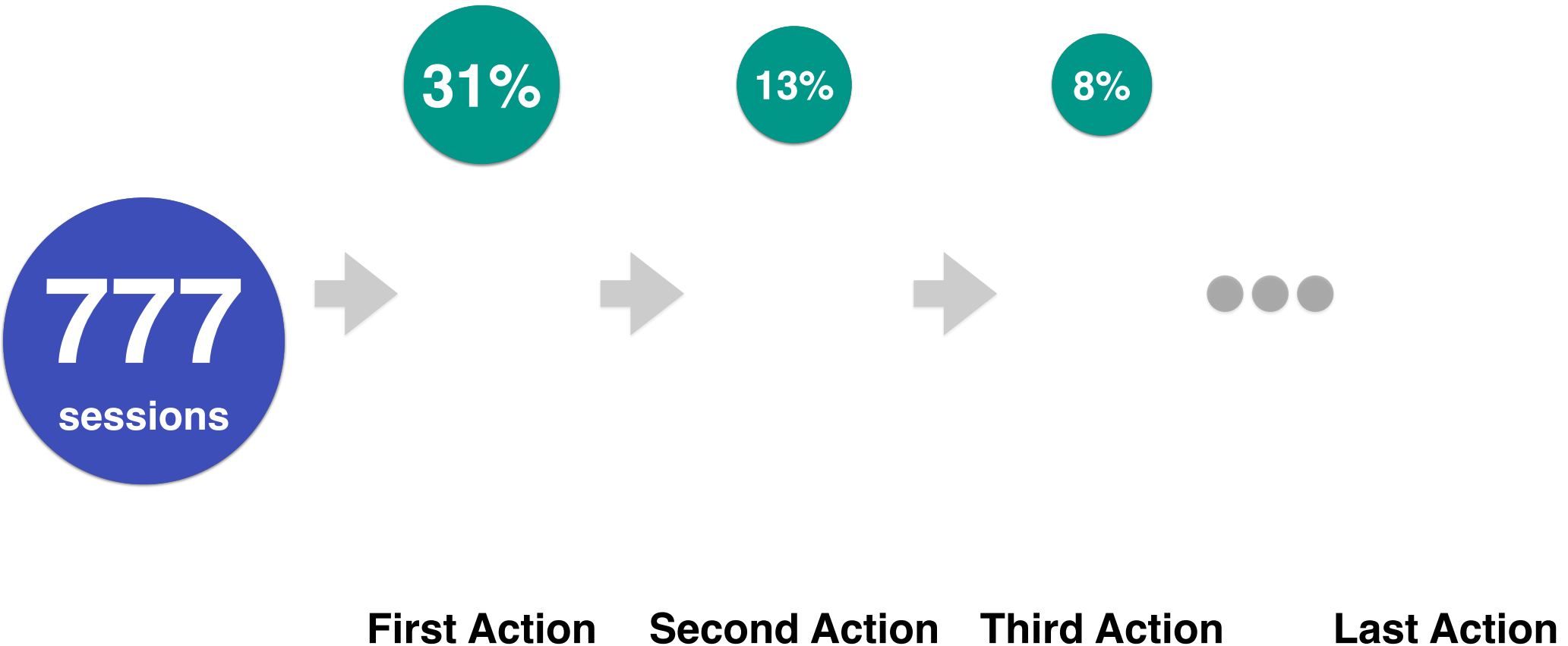
One hour time limit prevents return.

Honeypot Limitations

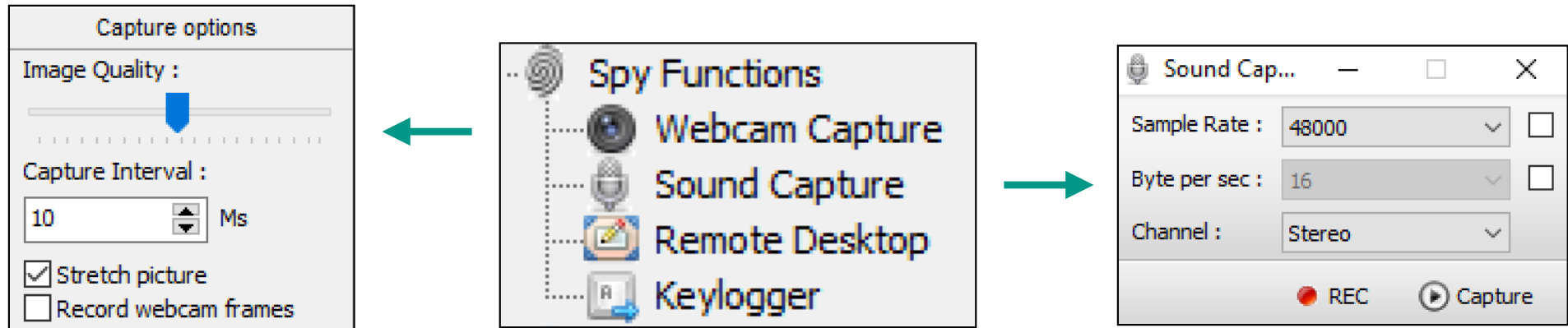
- No webcam or microphone feeds
- No responses to attacker-initiated chat, communication
- No keystrokes for keylogger
- Virtual machine indicators
- **Network containment policy**

Common Patterns of Action

● Webcam, Audio



(Attempted) User Monitoring



Webcam: **61%**

Microphone: **26%**

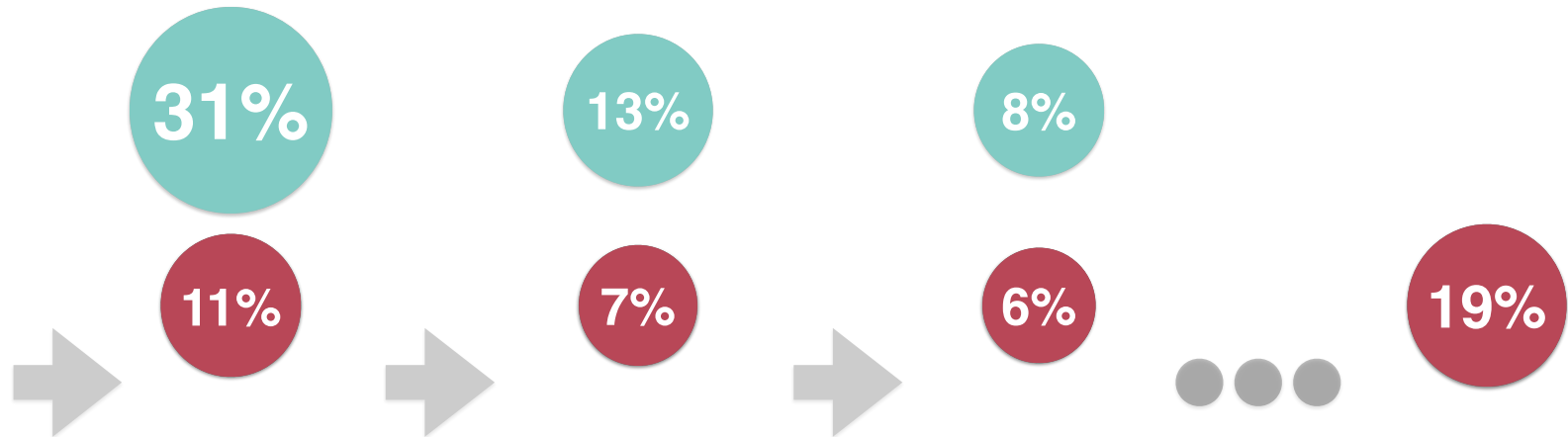
- Recall: We do **not** provide webcam / microphone feeds
- Motivation unknown!

Common Patterns of Action

● Webcam, Audio

● Passwords

777
sessions



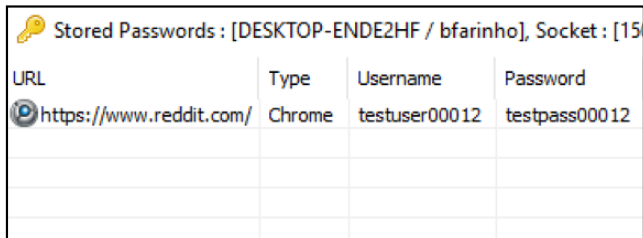
First Action

Second Action

Third Action

Last Action

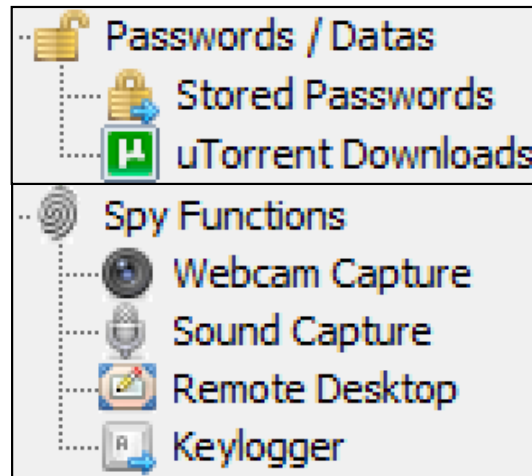
Credential Theft



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

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?

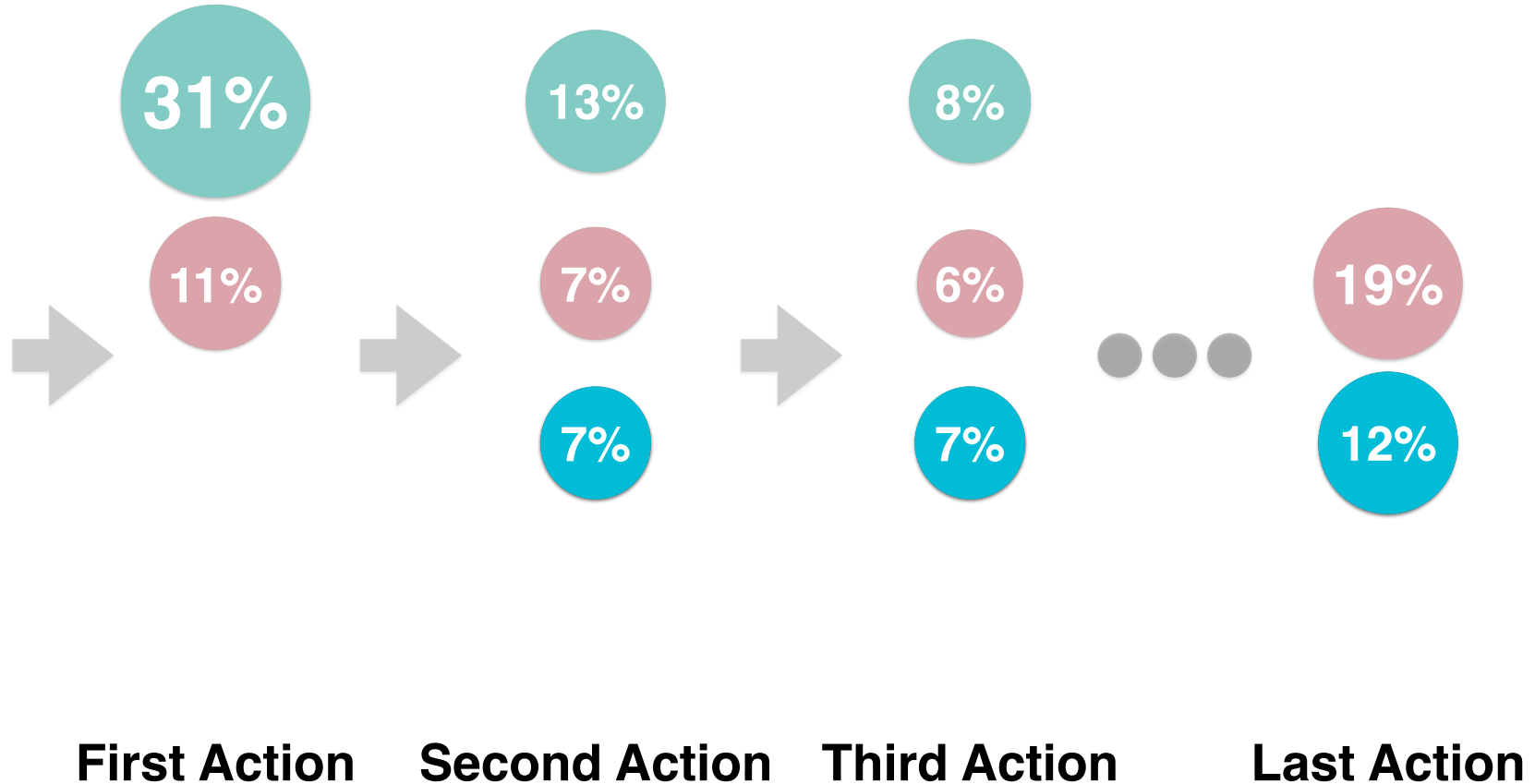
Common Patterns of Action

Webcam, Audio

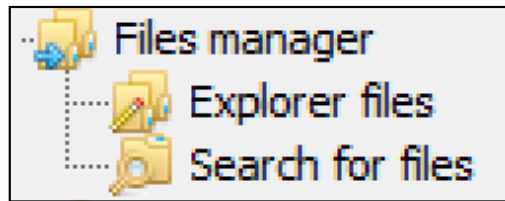
Passwords

Filesystem

777
sessions

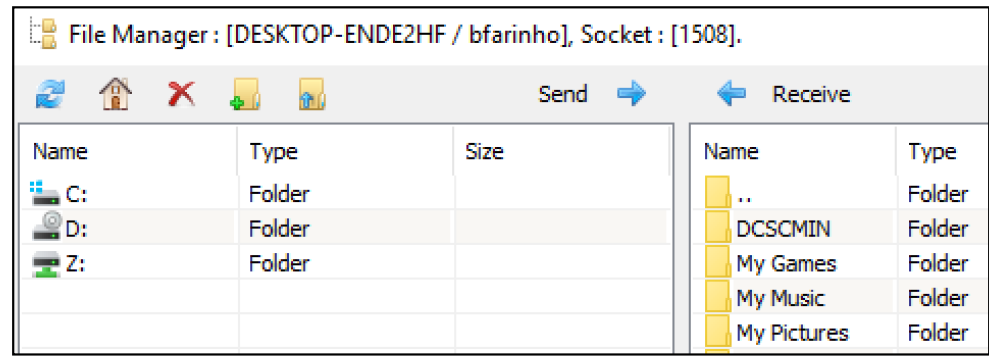


Filesystem Access



Filesystem

Exploration: **40%**



Upload: **18%**

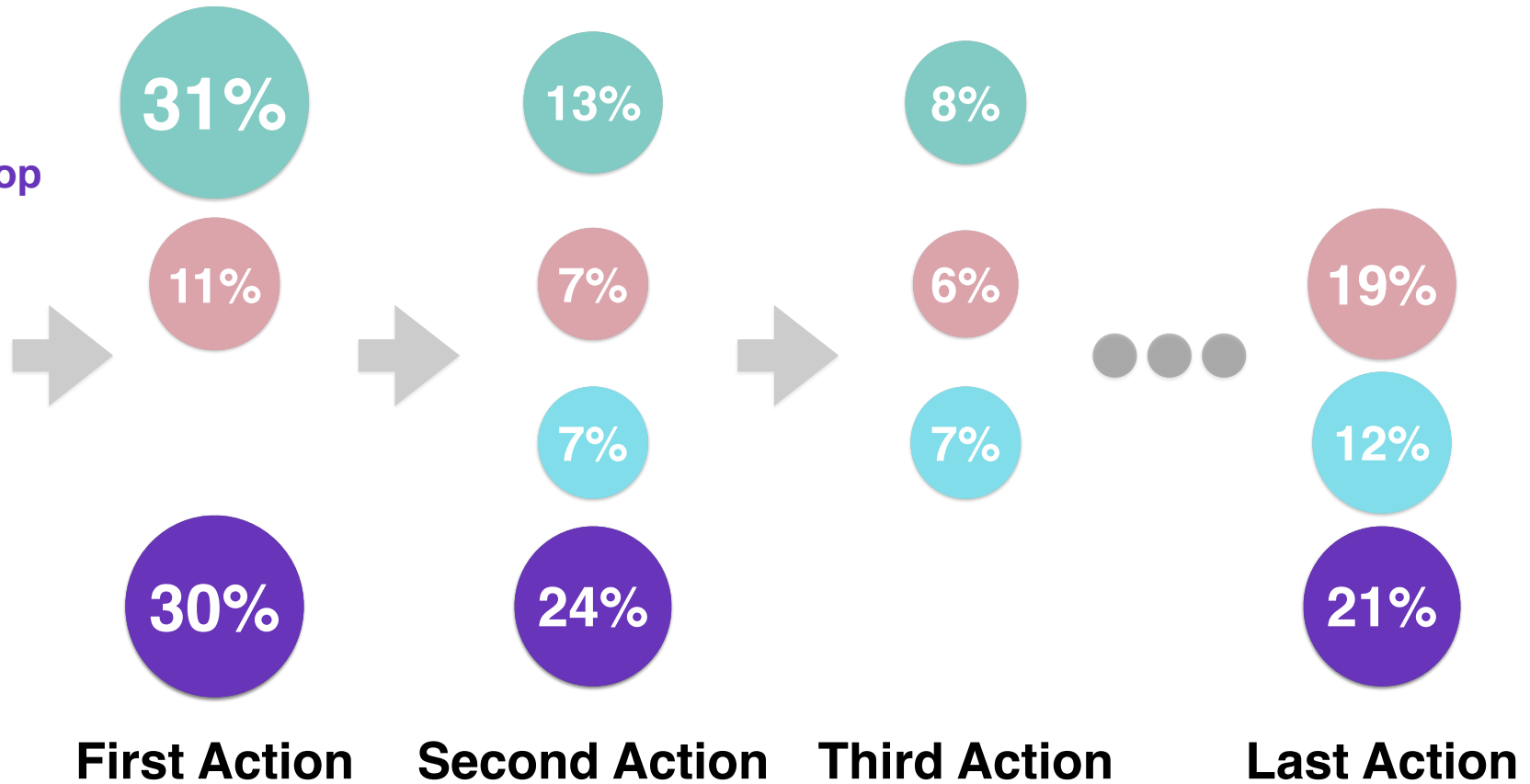
Download: **8%**

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

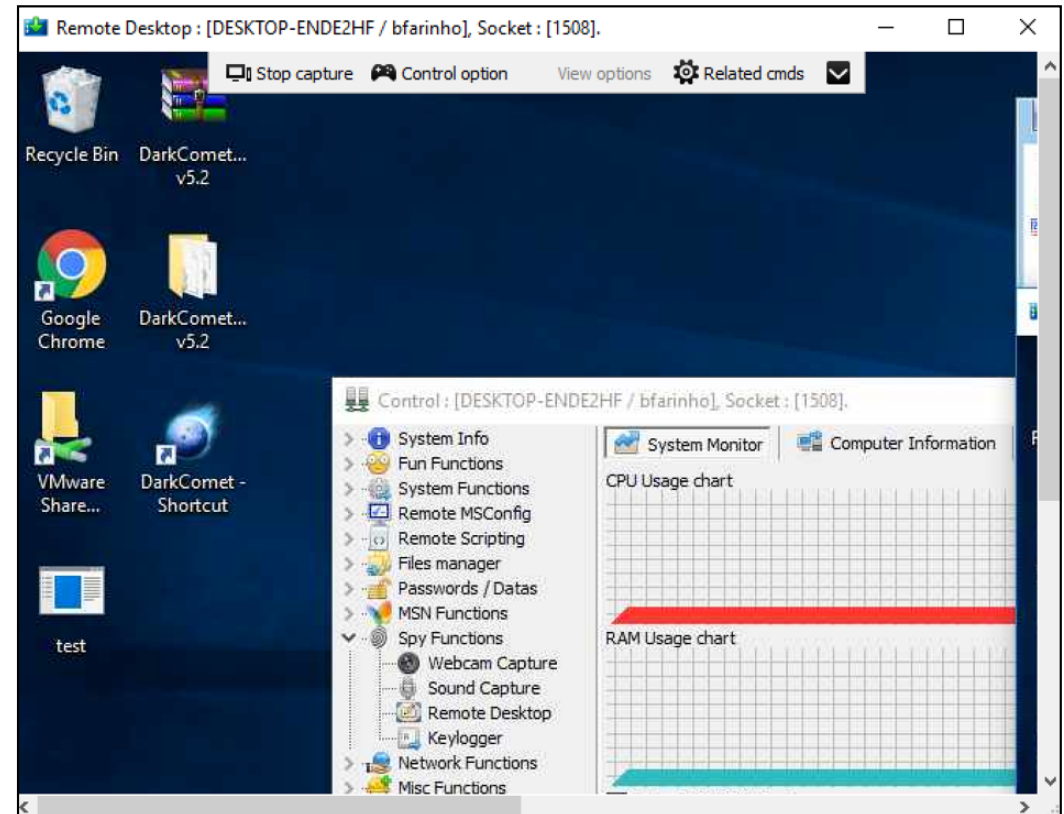
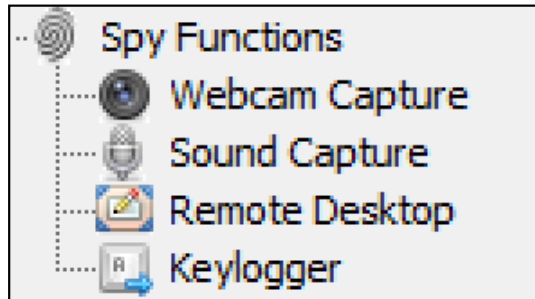
Common Patterns of Action

- Webcam, Audio
- Passwords
- Filesystem
- Remote Desktop

777
sessions



Remote Desktop

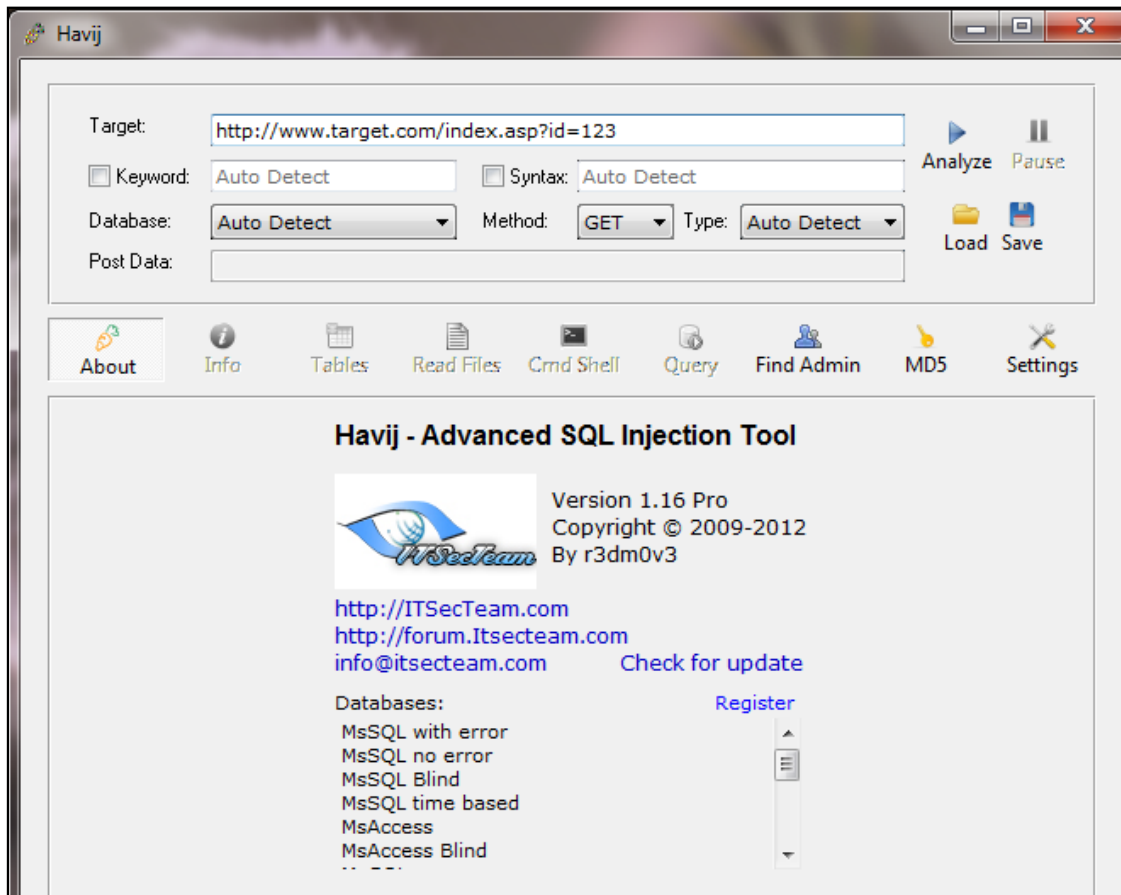


Remote Desktop: **83%** !

Active RD: **56%**

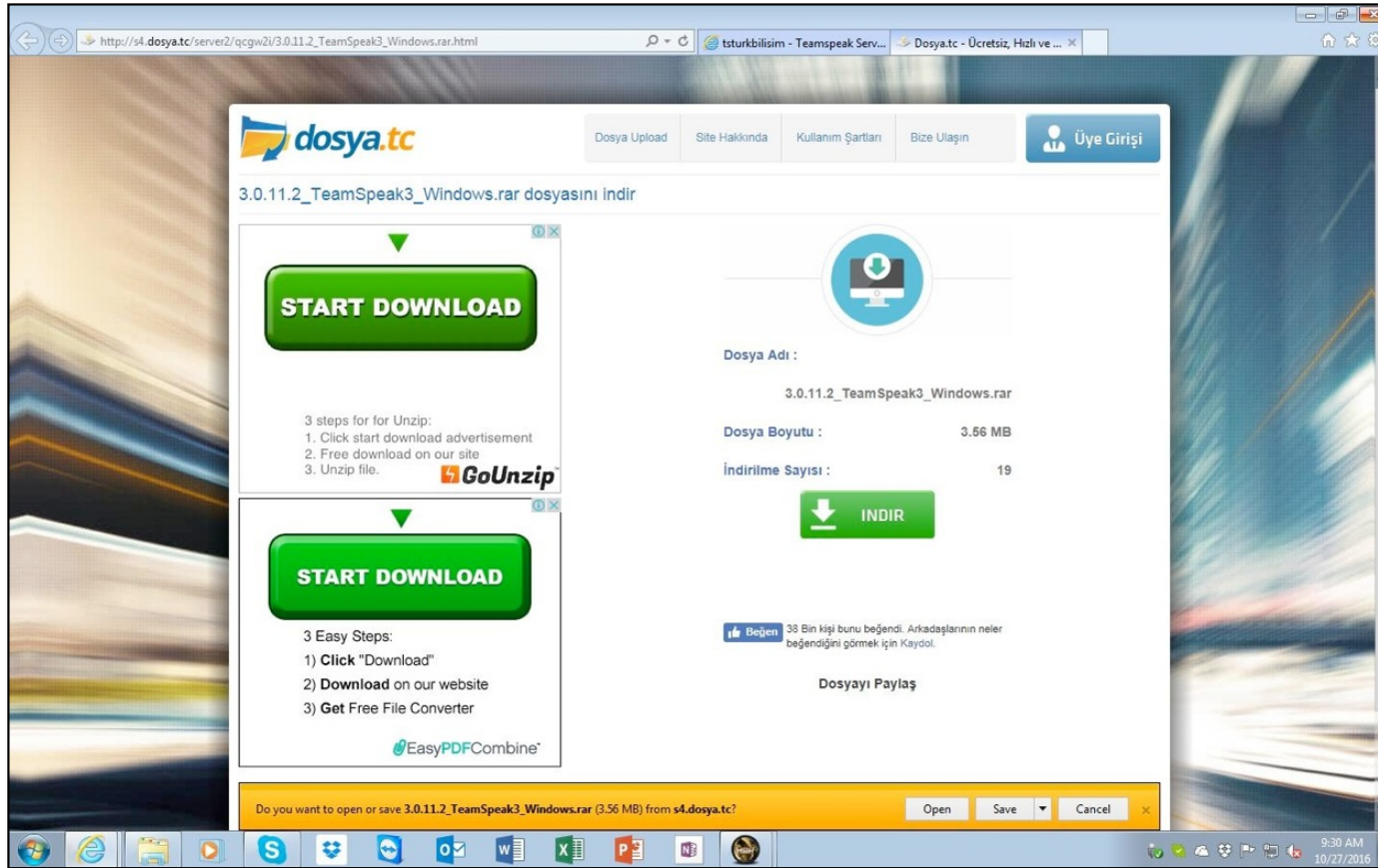
- GUI-based hacking tools
- Applications (Steam, browsers)

Remote Desktop



Havij SQL Injector

Remote Desktop

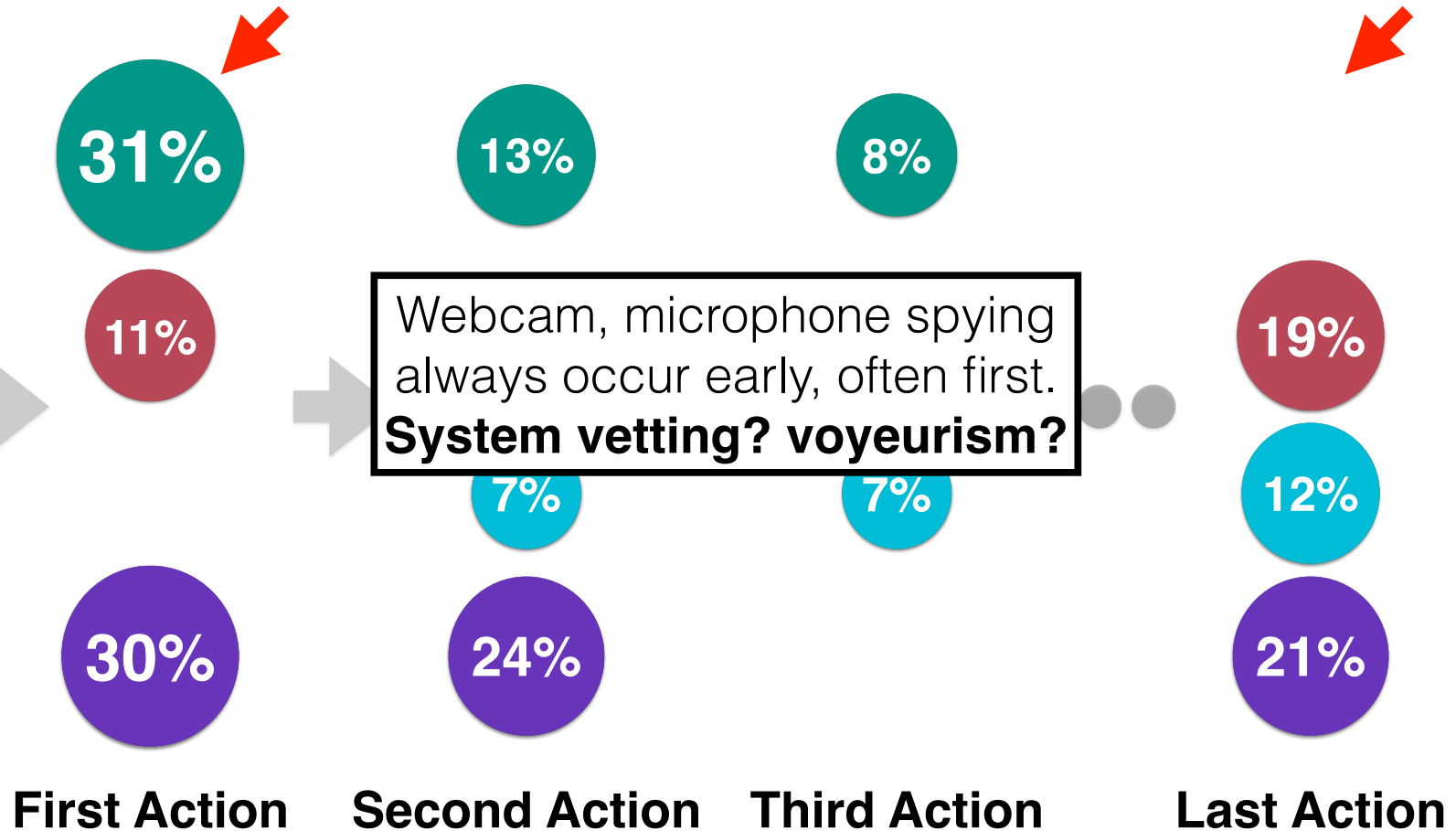


TeamSpeak 3

Common Patterns of Action

- Webcam, Audio
- Passwords
- Filesystem
- Remote Desktop

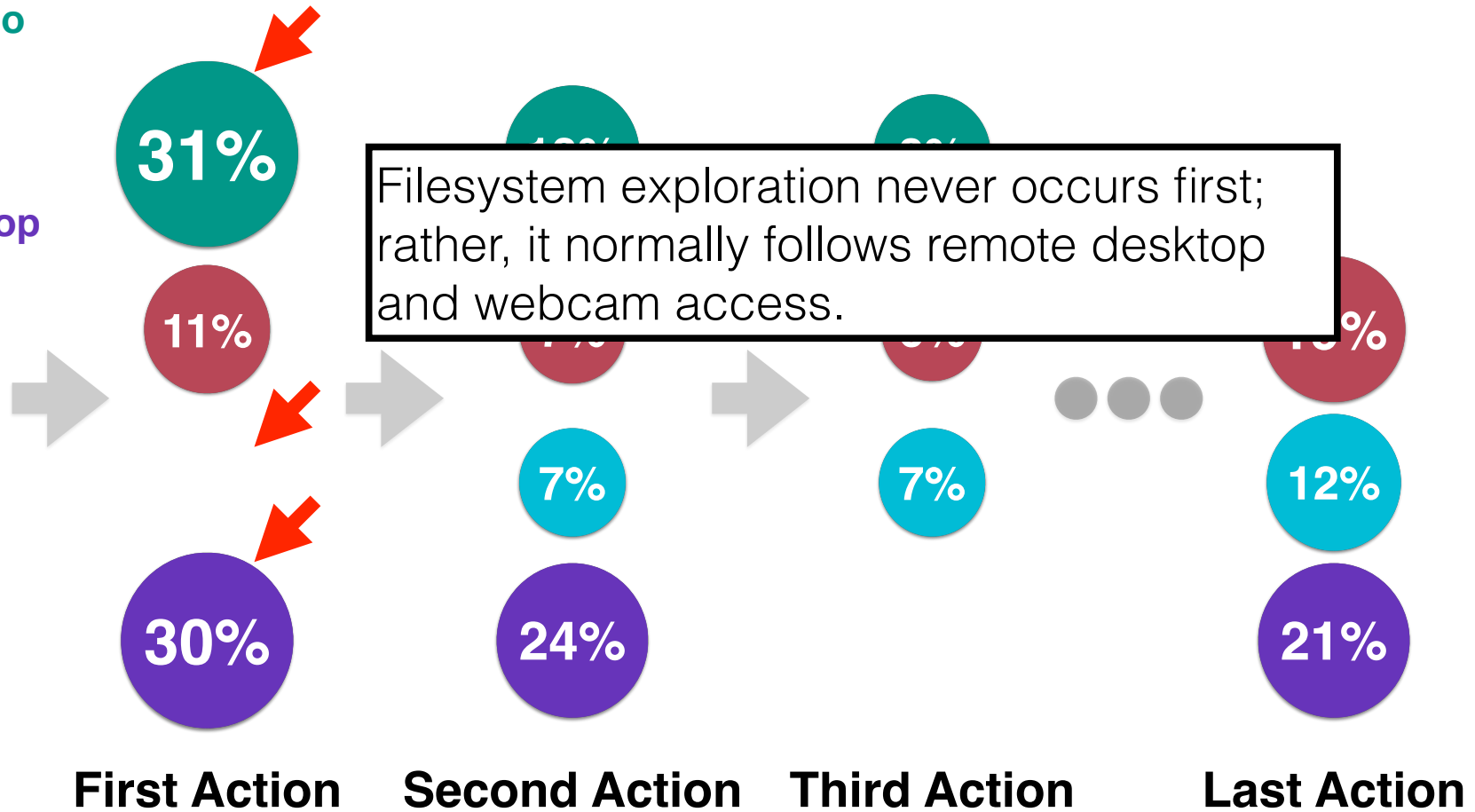
777
sessions



Common Patterns of Action

- Webcam, Audio
- Passwords
- Filesystem
- Remote Desktop

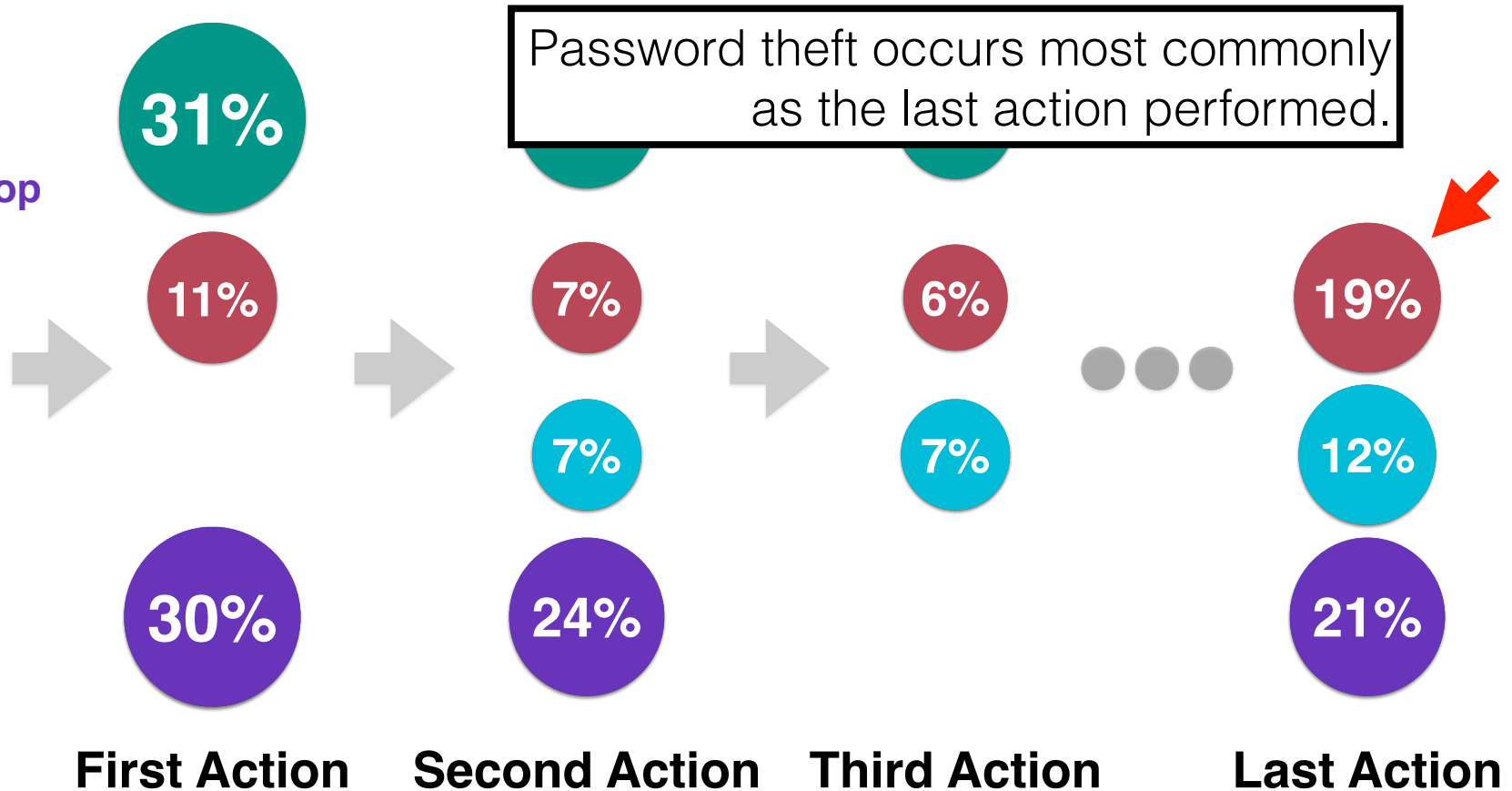
777
sessions



Common Patterns of Action

- Webcam, Audio
- Passwords
- Filesystem
- Remote Desktop

777
sessions

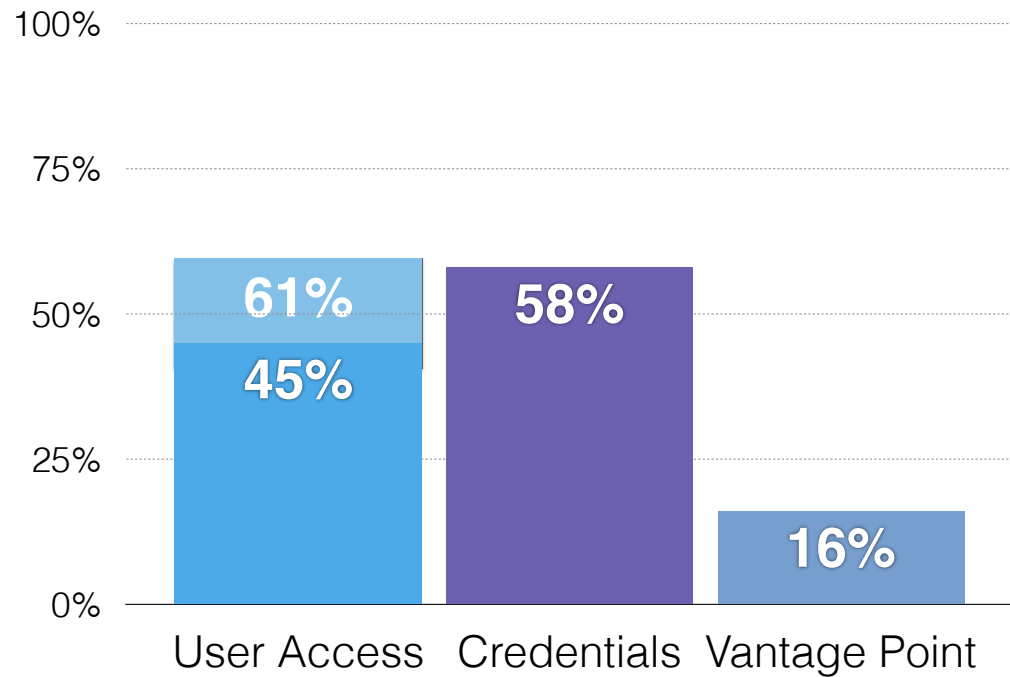


Overall Trends in Dataset



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

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



Further Research Questions



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

Tarpit Defense

- Average interaction: **4 minutes**
- Average remote desktop interaction: **7 minutes**
- **52.9** hours of interaction
 - Approximately 5 hours to create VM images
- **10,800** machine-hours of execution
- Honeypot realism cost-benefit



Engagement by Honeypot

