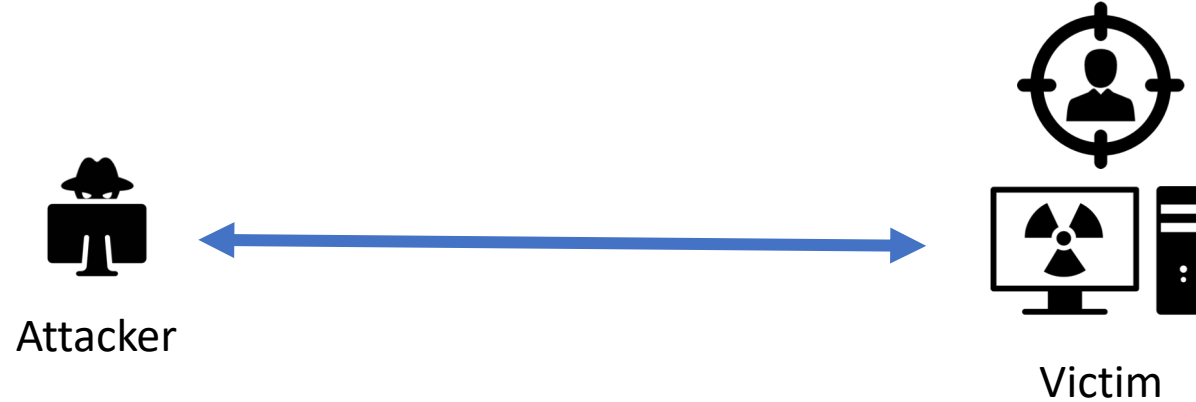


Schrödinger's RAT: Profiling the Stakeholders in the Remote Access Trojan Ecosystem

*Mohammad Rezaeirad, Brown Farinholt, Hitesh Dharmdasani,
Paul Pearce, Kirill Levchenko, Damon McCoy*



RAT: Remote Access Trojan

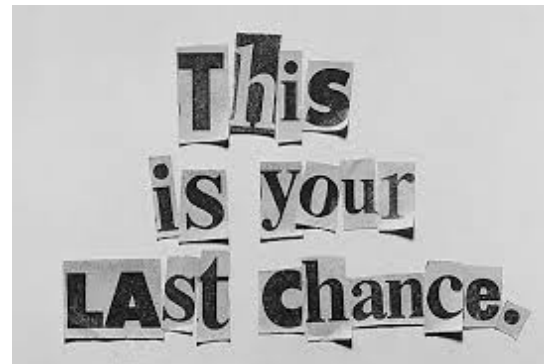


RAT: Attackers

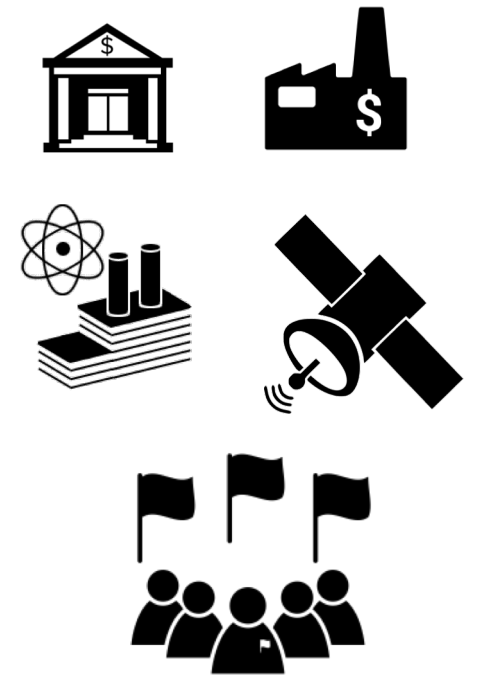
Script Kiddies



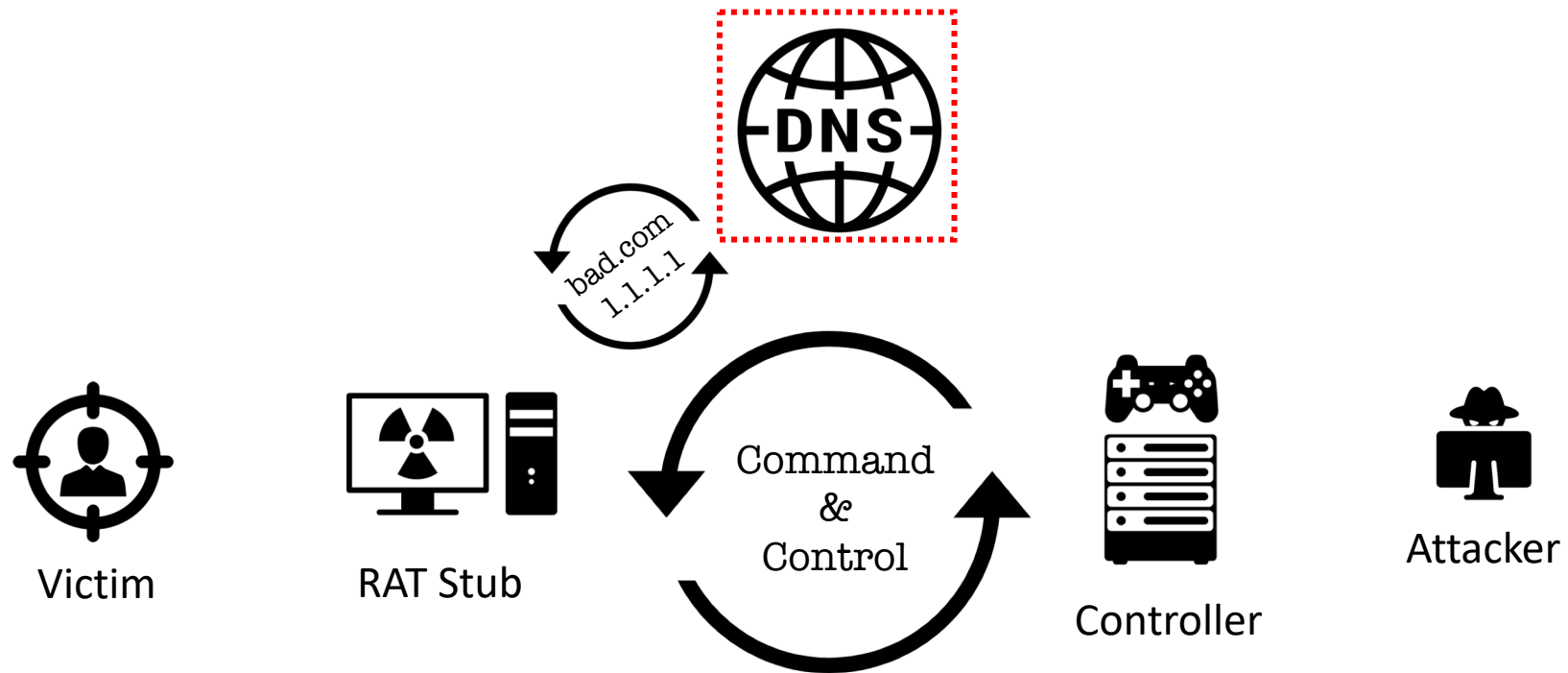
Blackmailers /
Voyeurs



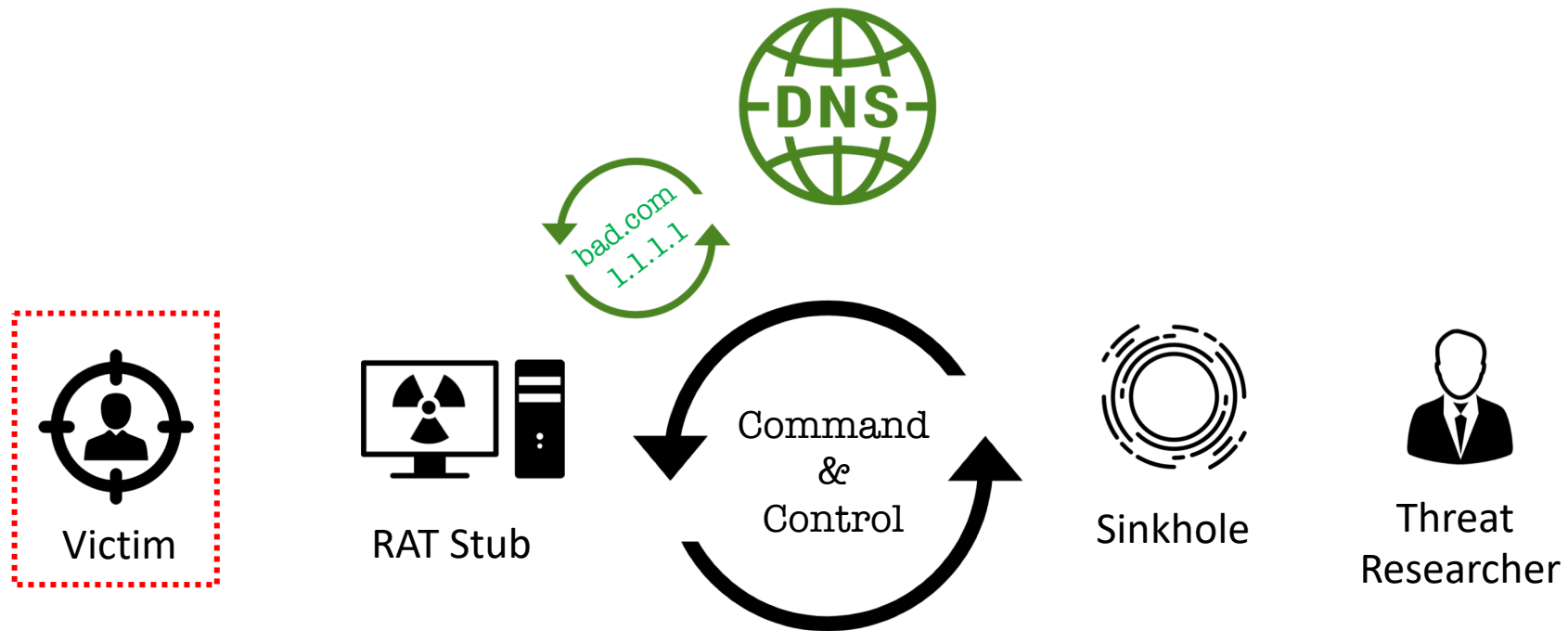
Nation State



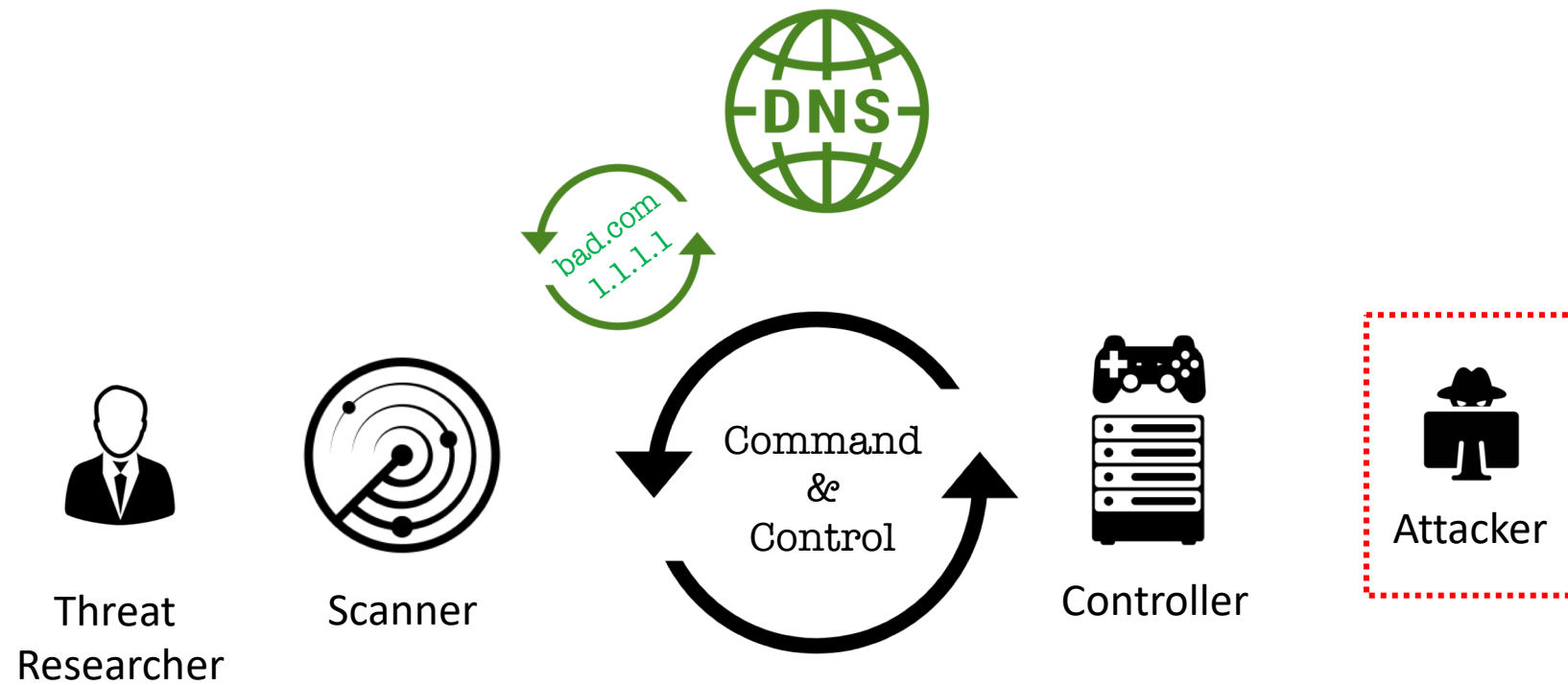
RAT: Basic Operation



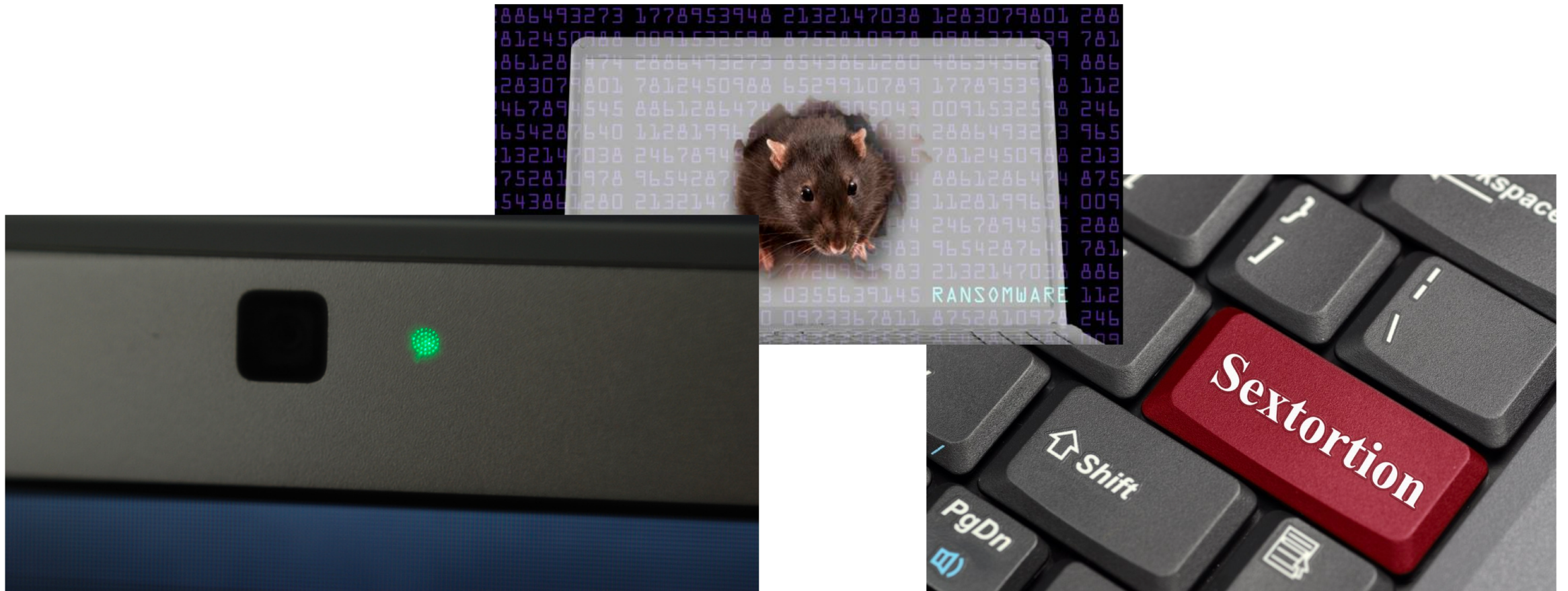
RAT: Sinkholing



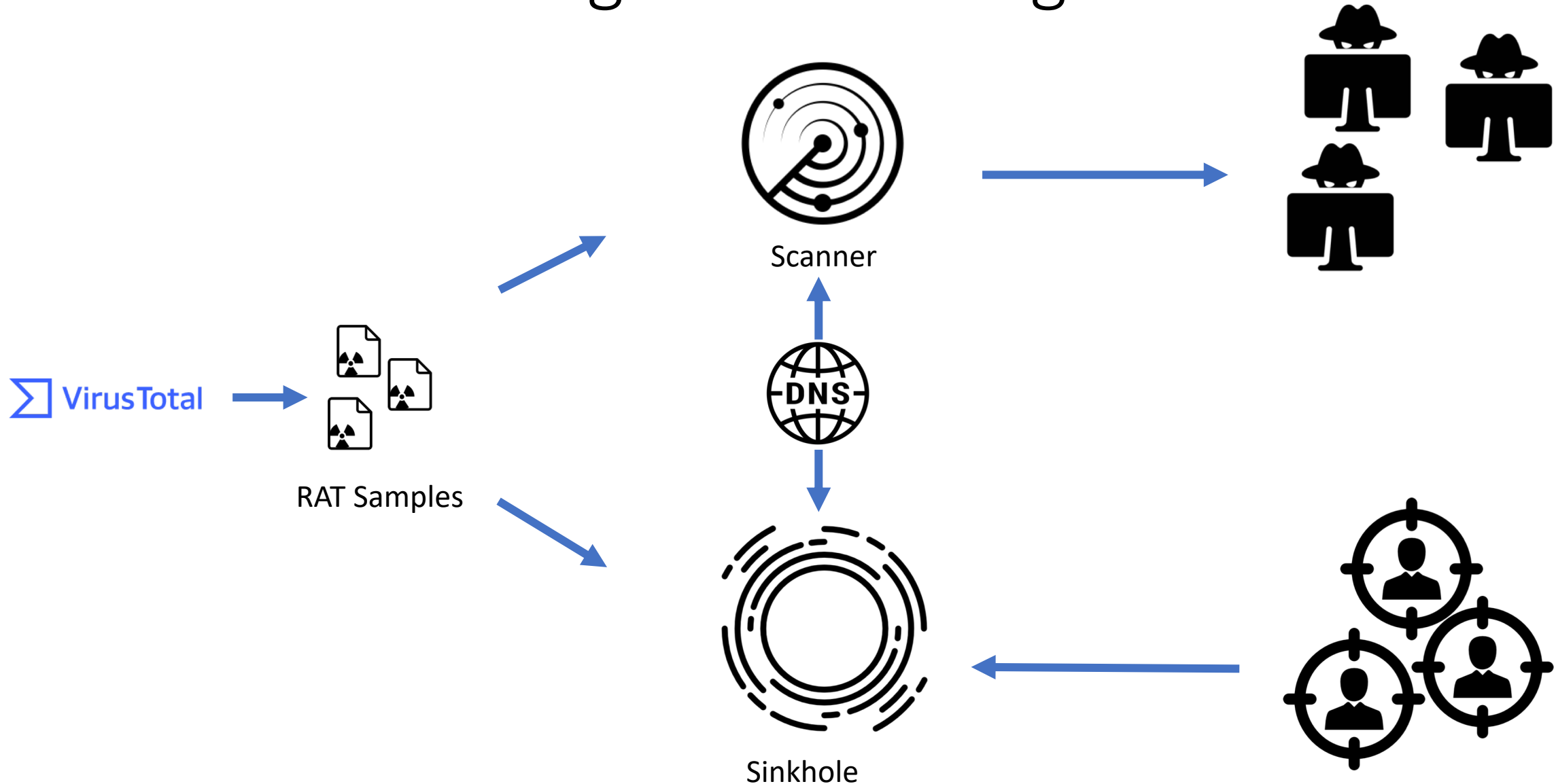
RAT: Scanning



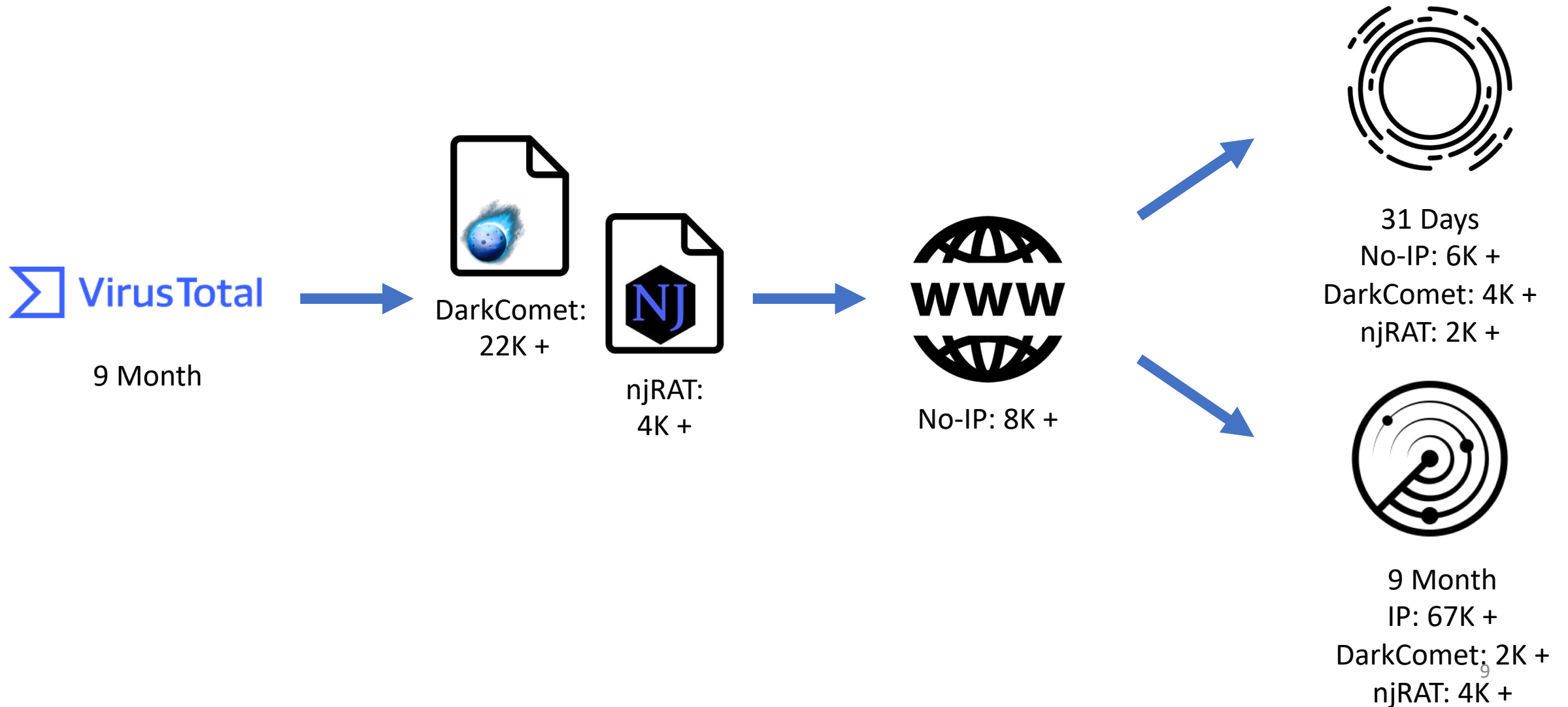
RAT Harms



Naïve Sinkholing and Scanning



Studying RAT Ecosystem: Data Set



To Whom It May Concern,

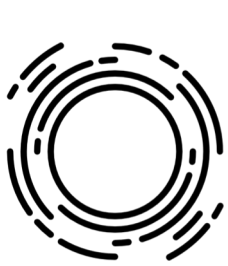
I am reaching out again to inform you that it appears that a vast majority of your servers, that are externally accessible, appear to contain evidence of malware installed that appears to be active and beaconing/communicating externally. The same website mentioned below in my previous email shows that 676 IPs that are registered to your University are potentially affected. I have attached screenshots of the results that are returned from shodan.io, but I would suggest that you or someone visit the site and check for yourself. The site is a well-known IoT scanner and is used by pen testers and Info Sec professionals alike. The site can be accessed at <https://www.shodan.io>. Once there perform a search for "category:malware". Once those results are returned, click on the "United States" under the "Top Countries" section on the left. As of this writing, George Mason University had the largest count of potentially infected IPs.

So far, it only appears that the RAT identified on all IPs is the NjRAT Trojan. I know that I don't have the familiarity of your network, however, this is something that should be looked into as this is only the surface. This could become a larger issues has the layers are pulled back.

The screenshot shows the Shodan search interface. The search bar contains the query "category:malware country:US". The results are displayed in a table with columns for IP address, host name, and location. The top result is 129.174.188.36, identified as George Mason University, located in Fairfax, United States. The second result is 129.174.188.20, also identified as George Mason University in Fairfax, United States. A map on the left shows the United States highlighted in red, indicating the location of the results.

| TOTAL RESULTS | IP Address | Host Name | Location |
|---------------|----------------|-------------------------|------------------------|
| 714 | 129.174.188.36 | George Mason University | United States, Fairfax |
| | 129.174.188.20 | George Mason University | United States, Fairfax |

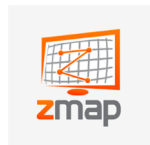
RAT-Hole: Initial Handshake Analysis



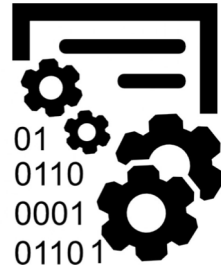
31 Days:
Conn: 153M +
~~IP: 828K +~~

Initial Handshake
Analysis:
IP: **12K +**

Unknown Or
Scanner: 816K +



RAT-Hole: Protocol Analysis



31 Days:
Conn: 153M +
~~IP: 828K +~~

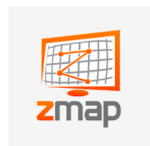
Initial Handshake
Analysis:
~~IP: 12K +~~

Protocol Analysis:

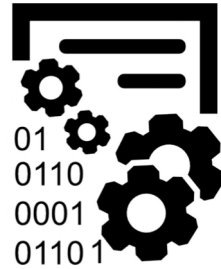
IP: **7K +**

Unknown Or
Scanner: 816K +

RAT Scanner: 5K +



RAT-Hole: Behavioral Analysis



31 Days:
Conn: 153M +
~~IP: 828K +~~

Initial Handshake
Analysis:
~~IP: 12K +~~

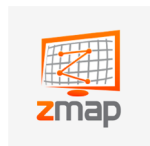
Protocol Analysis:
~~IP: 7K +~~

Behavioral Analysis:
Victim: **6K +**

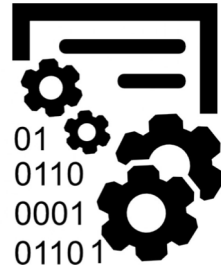
Unknown Or
Scanner: 816K +

RAT Scanner: 5K +

Sandbox: 1K +



RAT-Hole: Fingerprint Analysis



31 Days:
Conn: 153M +
~~IP: 828K +~~

Initial Handshake
Analysis:
~~IP: 12K +~~

Protocol Analysis:
~~IP: 7K +~~

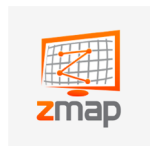
Behavioral Analysis:
~~Victim: 6K +~~

Fingerprint Analysis:
Victim: **3K +**

Unknown Or
Scanner: 816K +

RAT Scanner: 5K +

Sandbox: 1K +



Victim Analysis: Domains and Victims



Domain: 975

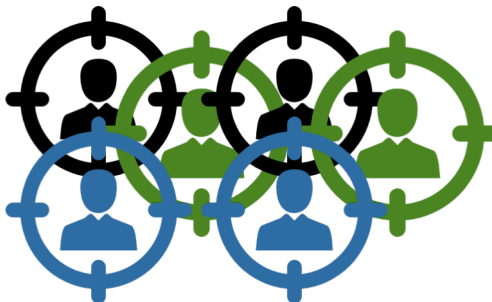
Single Victim: 43%



20 Victims: 90%



100> Victims: 3



Victim Analysis: Infection Longevity

- NO-IP Domains automatically expire after **30 days**
- 10% of Domains yielded Victims **150 days** after expiration
- Danger of domain **recycling**

Victim Analysis: Geolocation



Egypt:
njRAT: 94

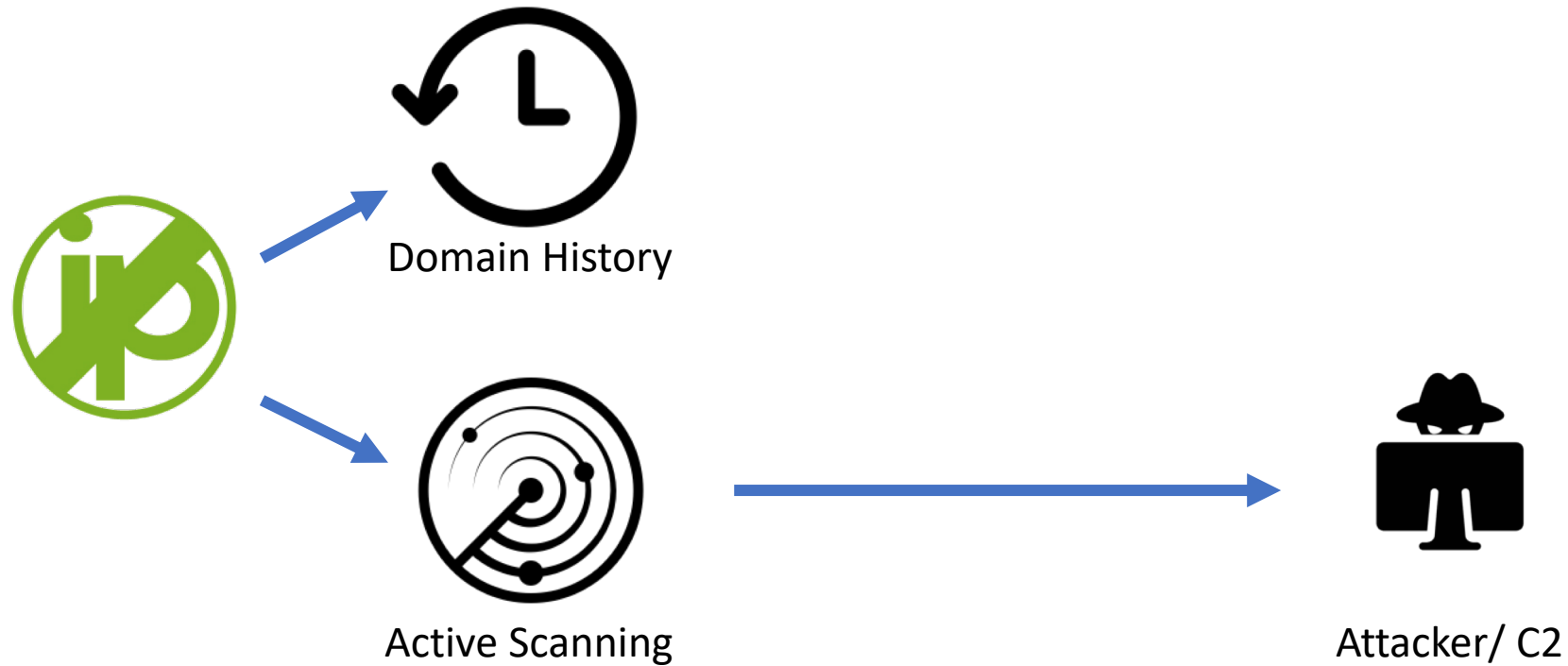


Brazil:
DarkComet: 1K +
njRAT: 178



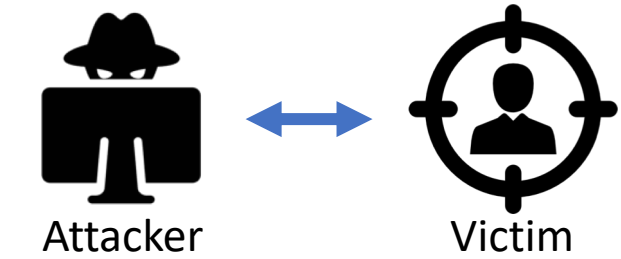
Turkey:
DarkComet: 130

RAT-SCAN: Measuring the Attackers




IPjetable
RELAXKS
40+%

Who Attacks Who?



Brazil



Brazil



Russia



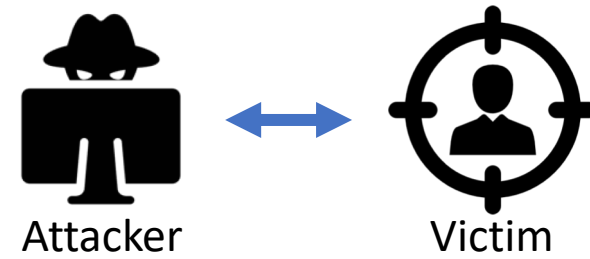
Russia



Turkey



Turkey



Russia



Ukraine



Russia



Brazil

Take-aways:

- There are other **Stakeholders** in RAT ecosystem
- You need methods to remove **Intelligence pollution** (~98%),
Otherwise conclusions are meaningless!
- There is RAT campaign **aftermath**

