

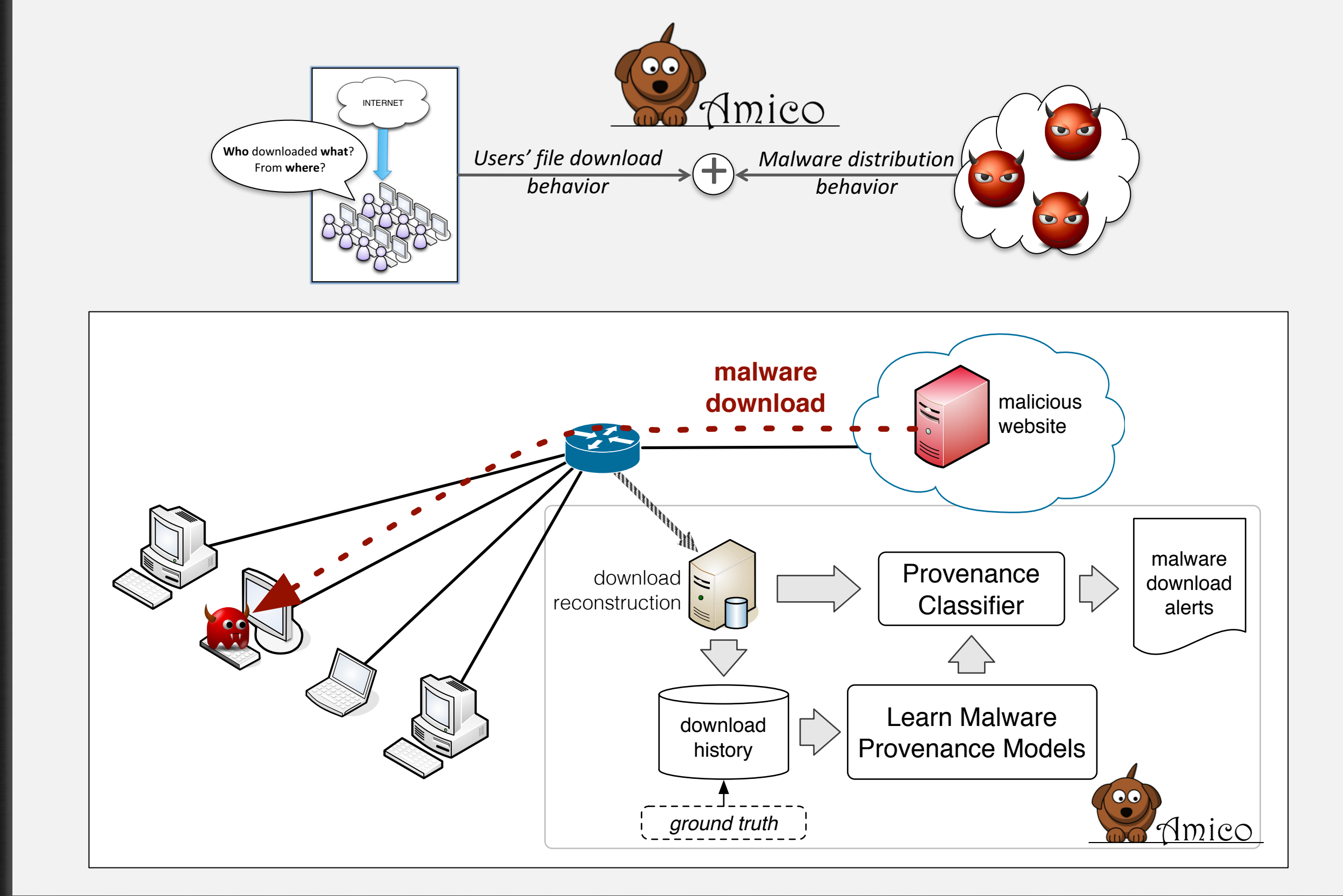
Need

- Sensitive networks are under constant threat from malware infections
- Malware can be used to open a backdoor and exfiltrate sensitive data
- Most networks still rely on signatures or blacklists, missing >65% of new threats
- We need a *behavior-based* approach that can *adapt to each specific network and detect never-before-seen malware*

AMICO's Benefits

- Turns attackers' malware distribution strategies into an advantage for defenders
- Complements signatures and blacklists
- Completely open-source

Approach and System Overview



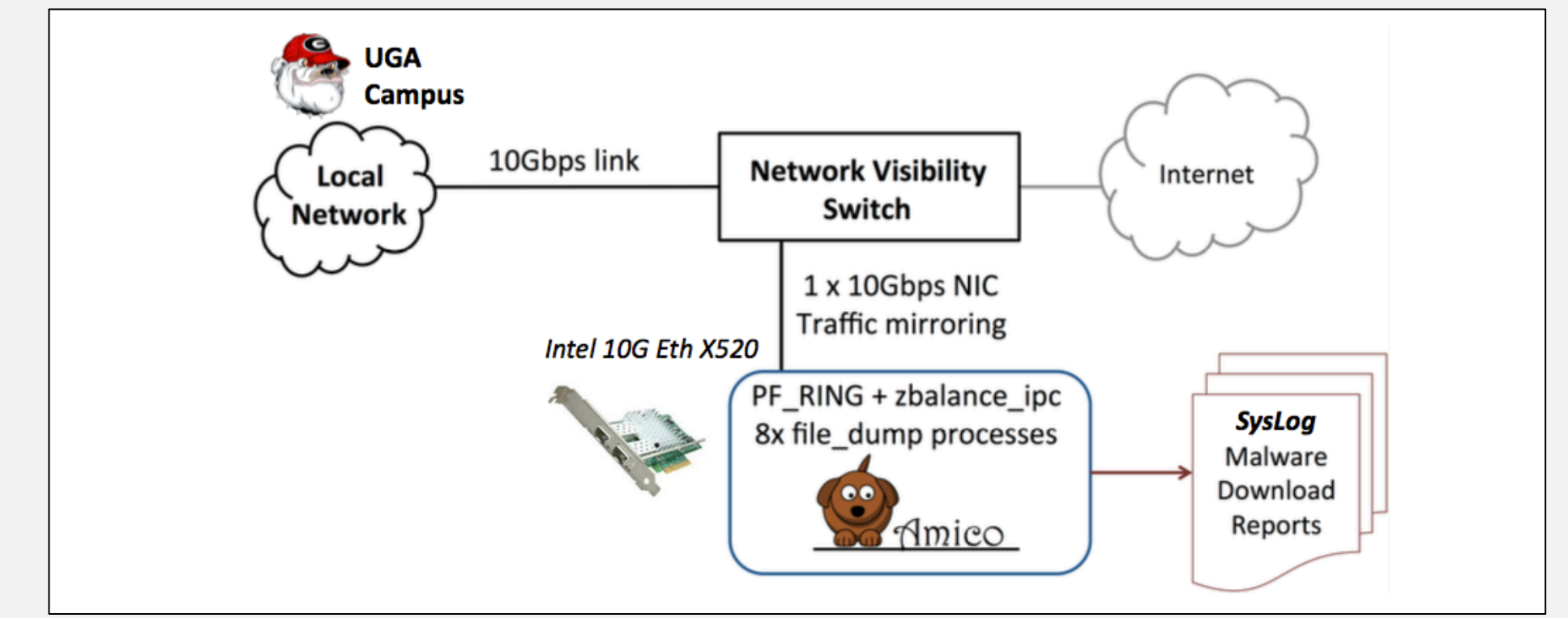
Modeling

Intuition: malware distribution is highly "agile"


	Malware	Benign EXEs
File content	changes frequently	is very stable
Domain names	change frequently	are very stable
IPs	change somewhat frequently	are relatively stable

- Statistical Feature:**
- Past file downloads info
 - Domain features
 - Server IP features
 - URL features, etc.

Deployment Overview



Pilot Results



Thousands of users

Example Syslog Report

Apr 14 09:24:56 netbox2 start_amico.py:
file download -- timestamp: 2017-04-14 09:23:46
client_ip: 172.21.x.x, server_ip: 45.79.194.109
server_port: 80, host: downloads.tweakbit.com
url: /go/src_ep_cnet_optimizer_PCR_3steps_970x66_v1/en/setup.exe
referrer: None
sha1: dff9f365b4d7b2e330e7c41bfd1e9697438bb77
md5: 1d20c15cf31e40fad73383d05321d149
file_size: 356864
av_labels: None
corrupt: False
file_type: EXE
amico_score: MALWARE#0.792

March 1 – April 15, 2017

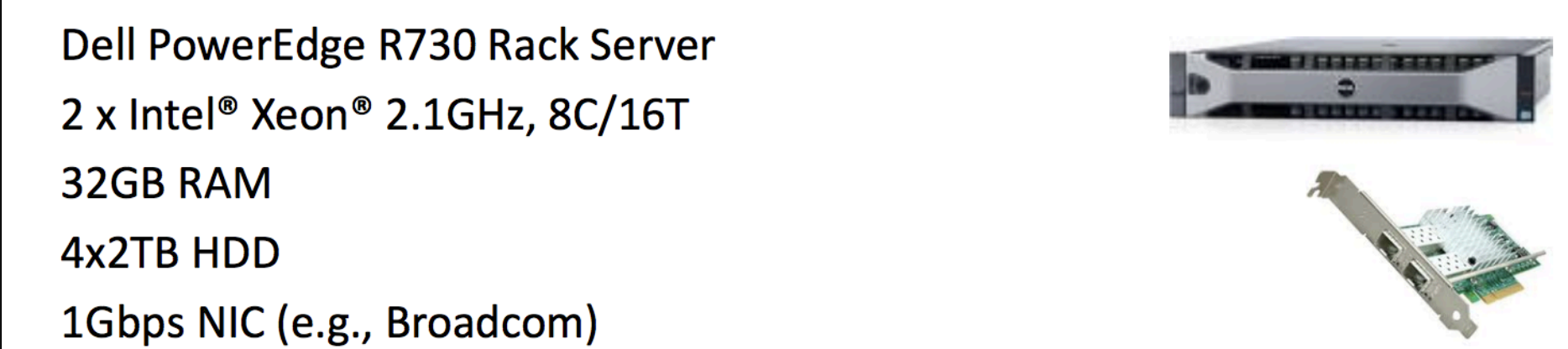
- Detected **1,183 malicious downloads** (AMICO Score > 0.7)
 - Clients: 844 distinct IPs
 - Downloads: 1,078 DMG, 87 EXE, 17 APK, 1 JAR
 - Files: **96 DMG, 58 EXE, 10 APK, 1 JAR**
 - False Alerts: 9 downloads (7 EXE, 1 DMG, 1 APK)
 - Still Unknown to VT: 55 downloads
 - **18 confirmed "Zero Days"** (previously unknown to VT)

Example of Pilot System Configuration

Dell PowerEdge R730 Rack Server
2 x Intel® Xeon® 2.1GHz, 8C/16T
32GB RAM
4x2TB HDD
1Gbps NIC (e.g., Broadcom)
1 x Intel 10G Eth X520 DP SPF+
Linux OS (e.g., Ubuntu Server 16.04)
PF_RING + 10G Intel ZC driver (free for EDU)

Recommended num. of CPU cores = Your Gbps of traffic X 2
– E.g., if you have 6Gbps of traffic, use 12 CPU cores

Operational Skills: Linux sys/network admin skills needed for deployment



< \$6,000

TTP - Next Steps

- Looking for partners to improve AMICO and make it widely adopted
- Pilot deployments in other large networks