Recently Published Research Poster – DScope: A Cloud-Native Internet Telescope

Reference: Eric Pauley, Paul Barford, Patrick McDaniel (2023). DScope: A Cloud-Native Internet Telescope. USENIX Security 2023.

Paper Link: https://www.usenix.org/conference/usenixsecurity23/presentation/pauley

Abstract:

Data from Internet telescopes that monitor routed but unused IP address space has been the basis for myriad insights on malicious, unwanted, and unexpected behavior. However, service migration to cloud infrastructure and the increasing scarcity of IPv4 address space present serious challenges to traditional Internet telescopes. This paper describes DScope, a cloud-based Internet telescope designed to be scalable and interactive. We describe the design and implementation of DScope, which includes two major components. Collectors are deployed on cloud VMs, interact with incoming connection requests, and capture pcap traces. The data processing pipeline organizes, transforms, and archives the pcaps from deployed collectors for post-facto analysis. In comparing a sampling of DScope's collected traffic with that of a traditional telescope, we see a striking difference in both the quantity and phenomena of behavior targeting cloud systems, with up to 450x as much cloud-targeting as expected under random scanning. We also show that DScope's adaptive approach achieves impressive price performance: optimal yield of scanners on a given IP address is achieved in under 8 minutes of observation. Our results demonstrate that cloud-based telescopes achieve a significantly broader and more comprehensive perspective than traditional techniques.

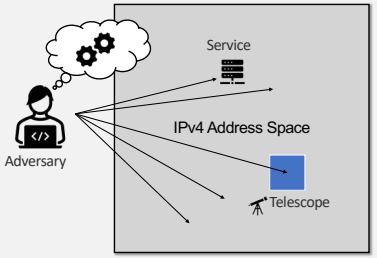
DSCOPE: A Cloud-Native Internet Telescope

Eric Pauley, Paul Barford, Patrick McDaniel
University of Wisconsin–Madison

MADS&P

MOTIVATION

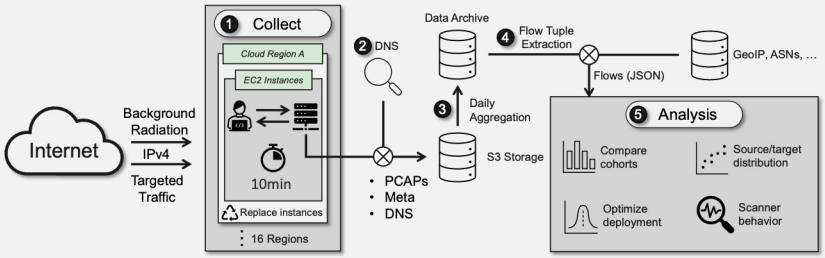
Adversarial Scanning on the Internet



- Internet-facing services are subject to constant attack as adversaries *scan* the IP address space.
- Existing vantage points have fixed footprints that may not be *representative* of traffic seen by real services.
- As deployments have shifted to public clouds, adversaries can *target* these and avoid measurement.

METHODS

A Global, Dynamic, Interactive Cloud Telescope



DSCOPE Design Goals:

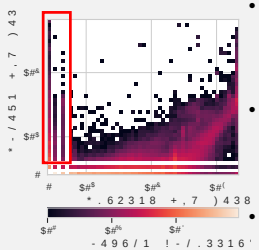
- Representative Traffic (Cloud IP Addresses)
- Interactivity (Application-layer Collection)
- Agility through the IP address space

DSCOPE Deployment by the Numbers:

- 2+ years of collected traffic
- 7.6M IPv4s
- 111k /24 networks

EVALUATION

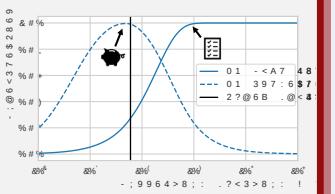
Comparing with Darknet Telescopes



- Traffic distribution shows that adversaries *target* services deployed on public clouds (red).
- Interactivity yields application-layer banner information and draws sophisticated adversaries.
- Large sample size allows for identification of ground truth data on service targeting.

Optimizing Collection Duration

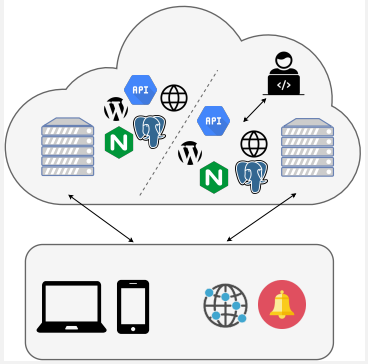
- IP addresses are near-completely measured in only 10^4s (3 hours) of observation.
- Optimal economic yield of phenomena occurs in only 10 minutes of measurement.



Result: short-measurement of **many** IPs is ideal!

APPLICATIONS

Measuring and Mitigating Risk of Cloud IP Address Reuse



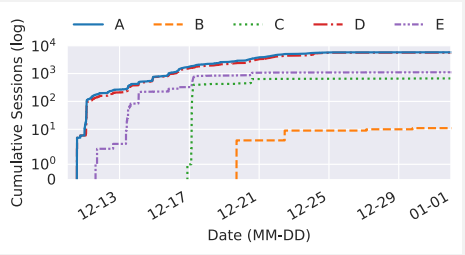
- Cloud providers reuse IP addresses after customers release them.
- Configuration linked to these IPs can remain.
- Clients connect and send sensitive information.
- Attackers allocate IPs and receive others' data.

DScope enables large-scale measurement of threats to cloud services by filtering received traffic for legitimate connections intended for previous cloud customers.

- 5,400 domains found vulnerable
- >5 million messages from cloud-managed services
- Sensitive data received: financial, personal, medical, etc.
- Disclosures/mitigations across industry/academic/government

Situational Awareness: Vulnerability Detection

DSCOPE receives targeted attacks from sophisticated adversaries. In 2021, DScope received some of the earliest-observed exploitation of the Log4Shell vulnerability (pictured).



DSCOPE also measures exploitation before existing sources such as the United States DHS's Known Exploited Vulnerabilities.

Application: DSCOPE provides security practitioners with situational awareness on real-world exploitation of vulnerabilities.

TAKEAWAYS

Internet deployment models have shifted

- Existing vantage points no longer see traffic from sophisticated adversaries.
- Organizations lack situational awareness and are at risk of attack.
- Cloud deployments bring new security and measurement challenges.

New vantage points yield practical security improvements

- Improved, more economical coverage of attacks against deployed services
- Coverage of sophisticated adversaries and application-layer behavior

Practitioners benefit from DSCOPE's new perspective

- Detected and mitigated risks to thousands of private/public organizations
- Provided rapid warning of emergent threats to deployed services

https://pauley.me
@EricPauley_
ericpauley
epauley@cs.wisc.edu