Mnemosyne: An Effective and Efficient Postmortem Watering Hole Attack Investigation System

Joey Allen, Zheng Yang, Matthew Landen, Raghav Bhat,
Harsh Grover, Andrew Chang, Yang Ji, Roberto Perdisci
Wenke Lee

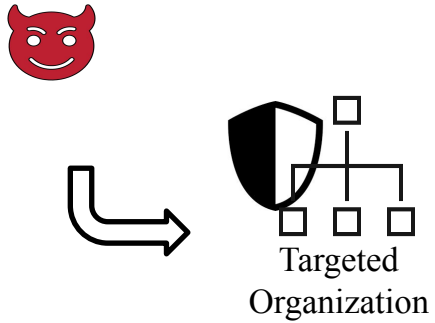
Watering Hole Attacks

Watering Hole Attacks

Adversary compromises a website routinely visited by targeted victims.

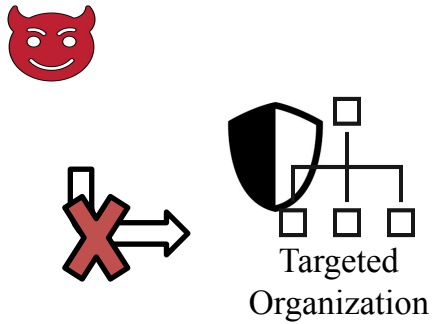
Watering Hole Attacks

Adversary compromises a website routinely visited by targeted victims.



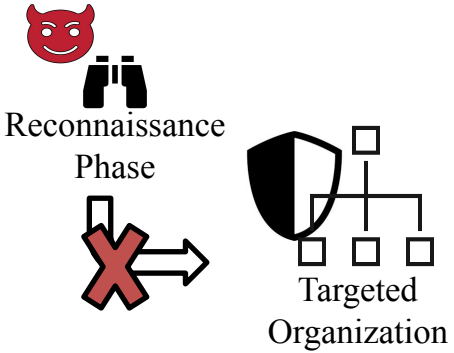
Watering Hole Attacks

Adversary compromises a website routinely visited by targeted victims.



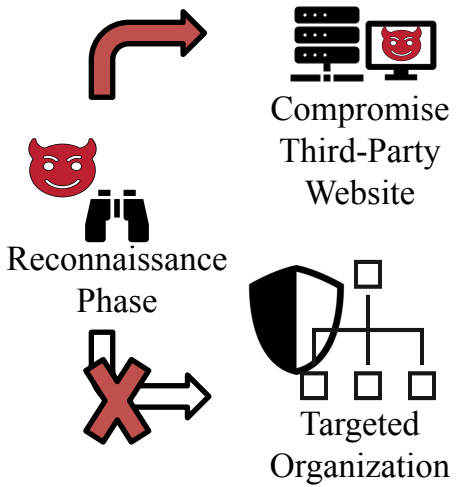
Watering Hole Attacks

Adversary compromises a website routinely visited by targeted victims.



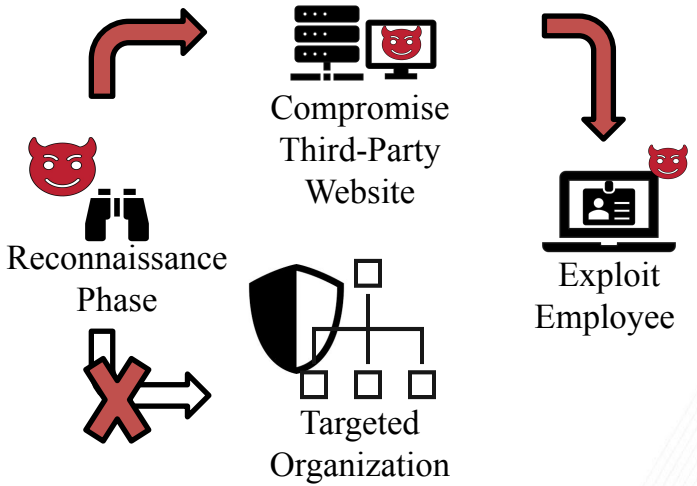
Watering Hole Attacks

Adversary compromises a website routinely visited by targeted victims.



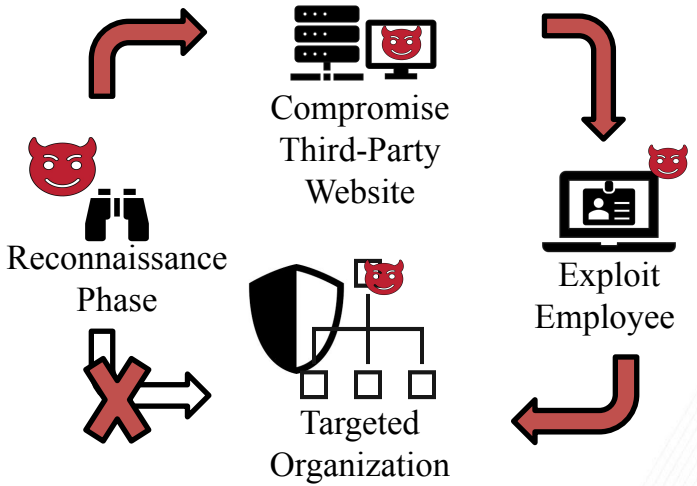
Watering Hole Attacks

Adversary compromises a website routinely visited by targeted victims.

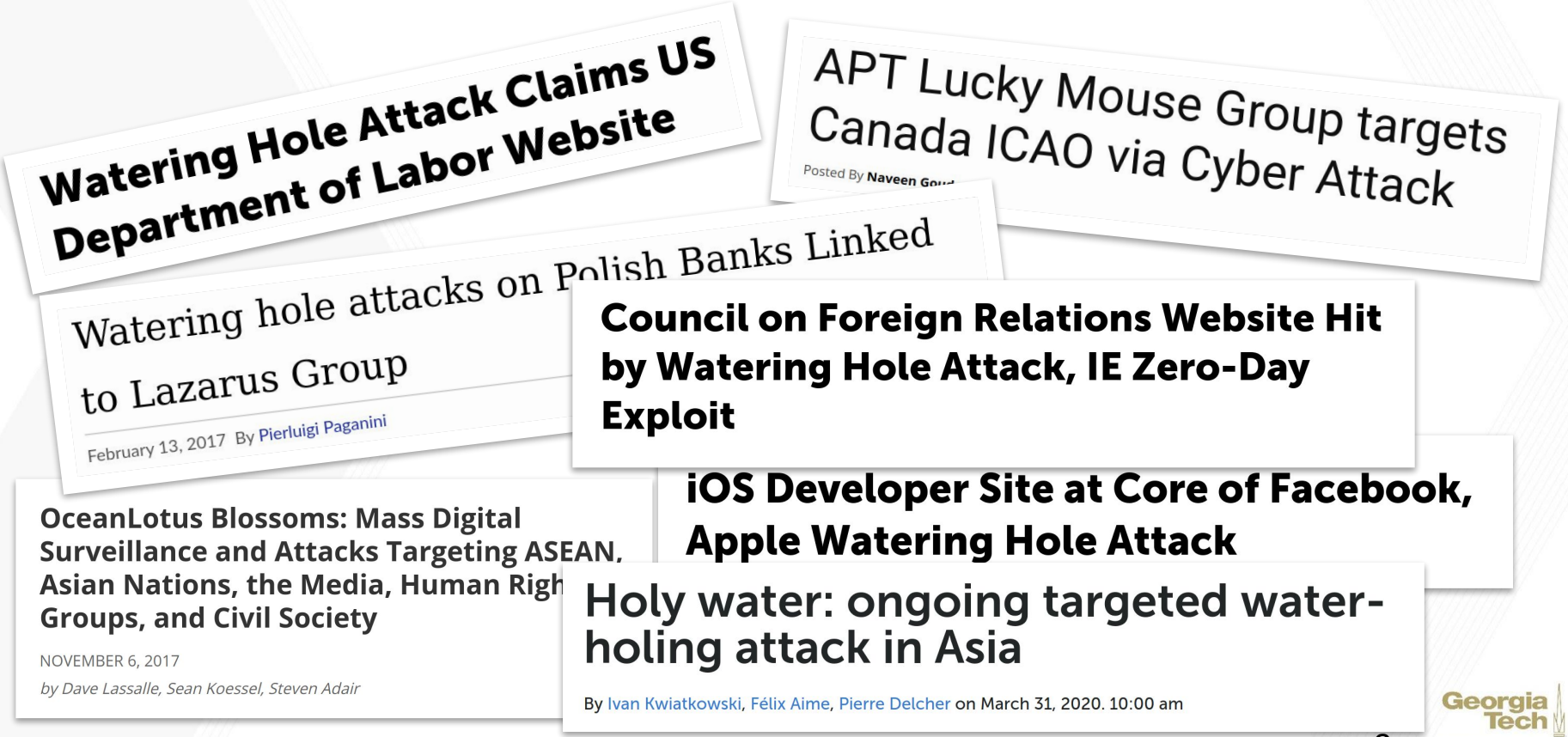


Watering Hole Attacks

Adversary compromises a website routinely visited by targeted victims.



Watering Hole Attacks in the Wild



Investigating Watering Hole Attacks

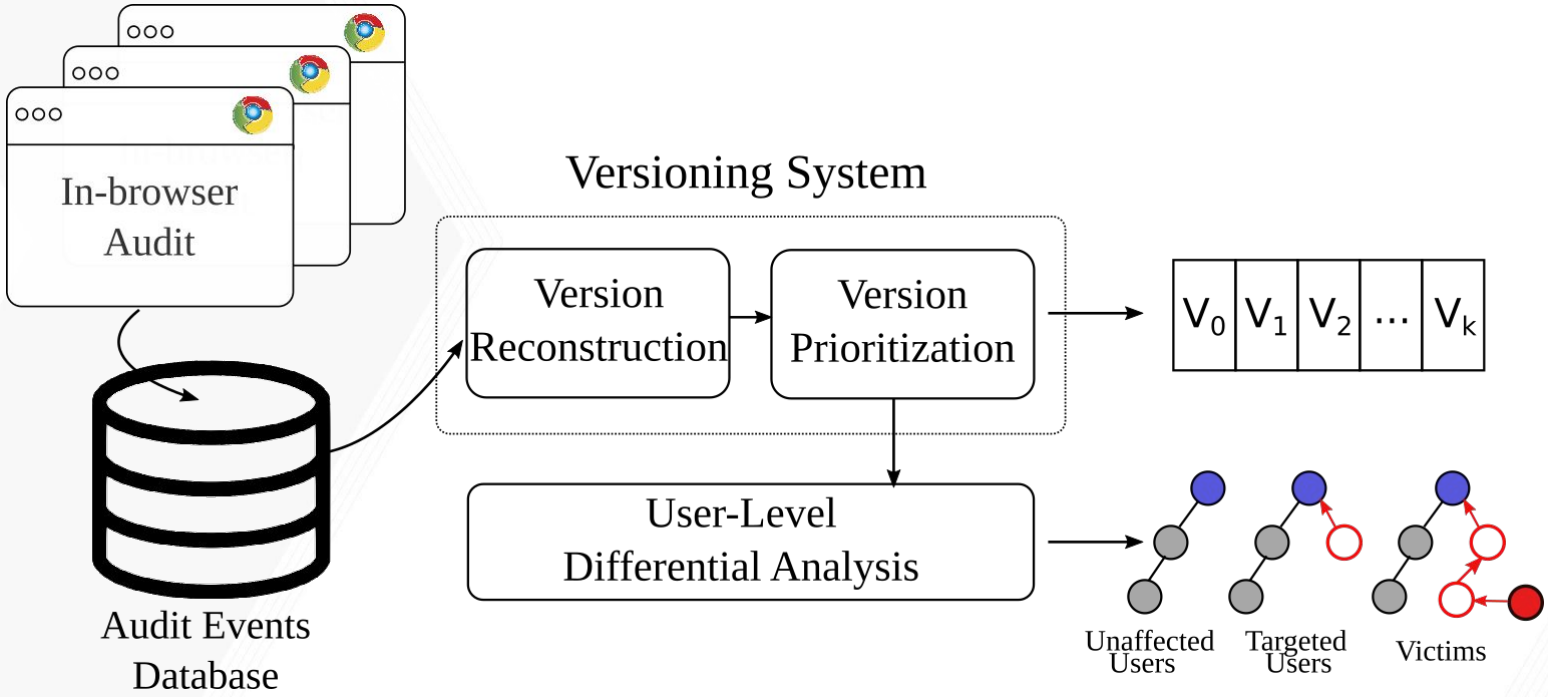
Cyber Threat Intelligence Report

Forensic Investigation

- What happened?
- When did the attack begin?
- Who was targeted?
- Where were the ramifications?

Mnemosyne

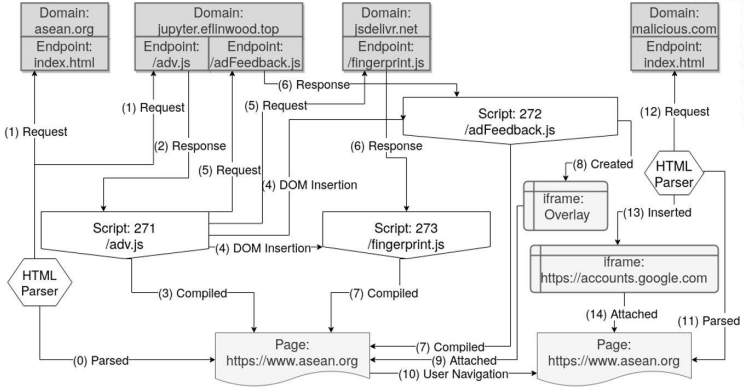
Mnemosyne (*nee-mos-uh-nee*) -- The Greek goddess of memory.



Browser Attack Provenance

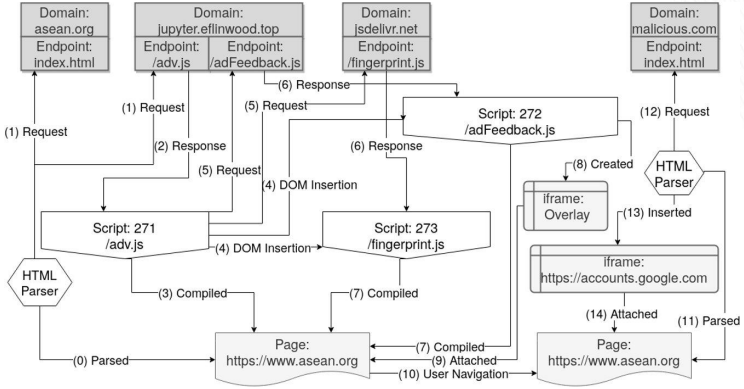
- **Browser Attack Provenance**
  - Nodes represent browser objects.
  - Edges represent causality relationships.

- Provides forensic analyst with capability to reconstruct web-based attacks.

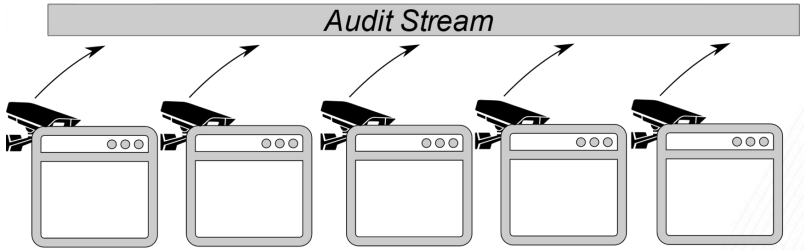


Browser Attack Provenance

- **Browser Attack Provenance**
  - Nodes represent browser objects.
  - Edges represent causality relationships.
- Provides forensic analyst with capability to reconstruct web-based attacks.



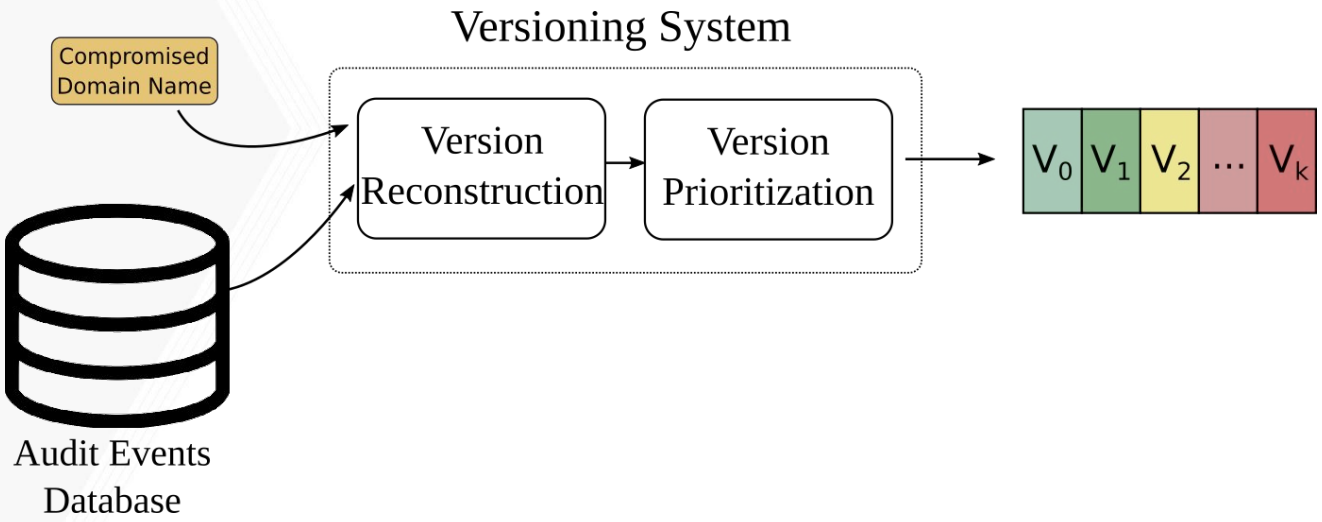
- **Auditing Daemon**
  - Collects browser audit logs.
  - Relies on existing DevTools APIs.



Versioning System

Purpose:

- Help the forensic analyst identify the window-of-compromise.



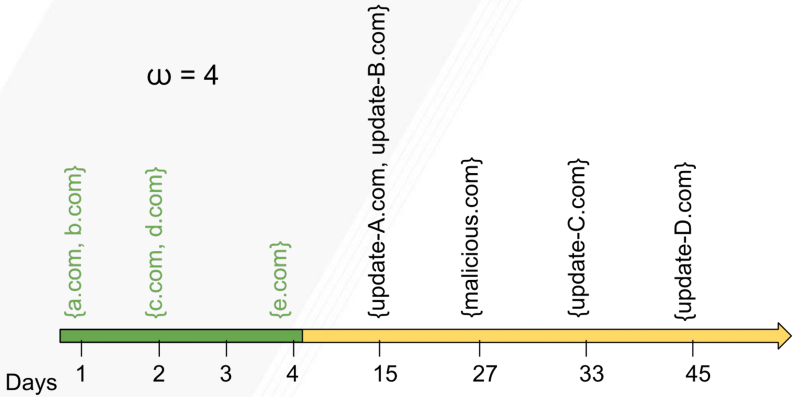
Version Reconstruction

Design Goals:

- Minimize the number of versions generated.
- Decouple benign and malicious modifications.

Our Approach:

- Domain Versioning System



Analysis Timeline

Version	Domains	Days
0	a.com, b.com, c.com, d.com, e.com	0-4
1	Update-A.com, Update-B.com	15
2	Malicious.com	27
3	Update-C.com	33
4	Update-D.com	45

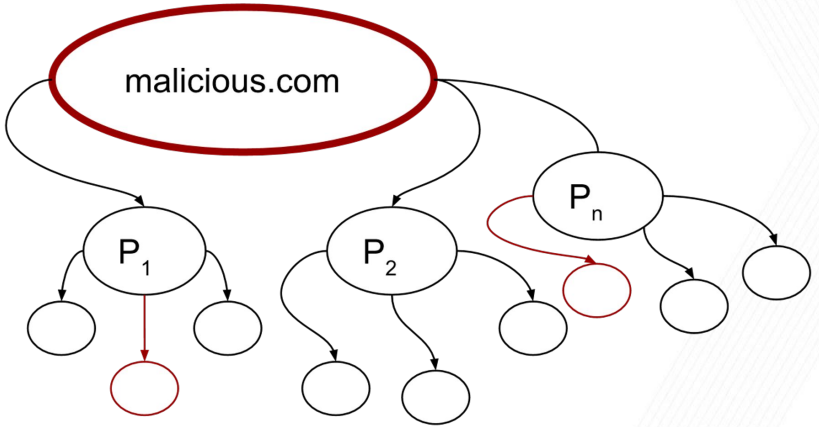
Version Report

Version Prioritization

Purpose:
- Prioritize versions based on suspiciousness.

Our Approach:
- Analyze versions independently.
- Identify suspicious behavior.
- Assign overall suspiciousness score.

Suspicious Events:
- TTPs provided by the MITRE ATT&CK Framework.



Version 2

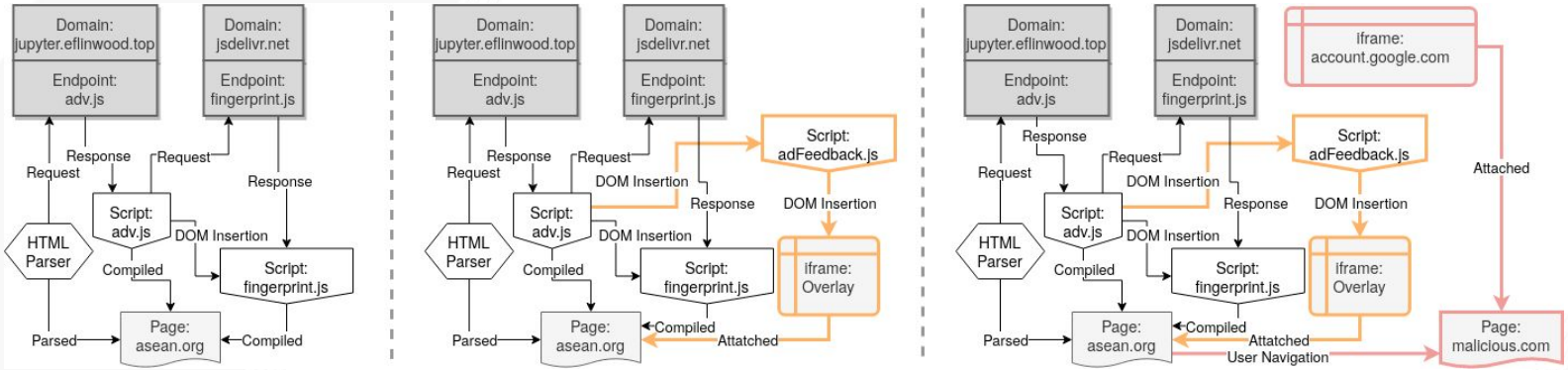
User-Level Analysis

Purpose:

- Identify targeted users and victims of the attack.

Approach:

- Analyze the most suspicious version.
- Generate user-level versions using differential analysis.



Dataset Evaluation

Evaluation: Data Collection & Datasets

- **Data Collection**
  - Developed a scalable watering hole testbed.
  - Simulates making malicious modifications to a website.
  - Simulates visiting a compromised website.
- **Attack Scenarios**
  - Simulated 7 attack scenarios.

Evaluation

- How effective is Mnemosyne at reducing the analysis scope of the forensic investigation?

- How does the benign evolution of websites affect Mnemosyne's analysis?

- What is the runtime and storage overhead of Mnemosyne?

Evaluation: Effectiveness

- How much of the analysis space does Mnemosyne reduce?
  - Analysis space: **Domains & Scripts**
- Mnemosyne reduced **99% of scripts** from analysis space on average.
- Mnemosyne reduced **98% of domains** from analysis space on average.

Analysis Fatigue

Evaluation

- How effective is Mnemosyne at reducing the analysis scope of the forensic investigation?

- How does the benign evolution of websites affect Mnemosyne's analysis?

- What is the runtime and storage overhead of Mnemosyne?

Evaluation: Benign Evolution

- **Purpose:**
  - Measure evolution of third-party websites.
- **Data Collection:**
  - Collected simulated visits to 1,830 websites.
  - Developed categories of websites.
  - February 6th, 2020 - August 18, 2020
- **Updates**
  - **Most Frequent:** News - 4.33 updates
  - **Least Frequent:** Games - 1.52 updates
  - **Alexa 1K:** 2.15 updates
- **False-Positive Analysis:**
  - 4.97% of benign updates were flagged as suspicious.

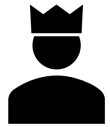

Government


Entertainment


Games


Business


Health


Politics


Shopping


News


Alexa 1k

Evaluation

- How effective is Mnemosyne at reducing the analysis scope of the forensic investigation?
- How does the benign evolution of websites affect Mnemosyne's analysis?
- What is the runtime and storage overhead of Mnemosyne?

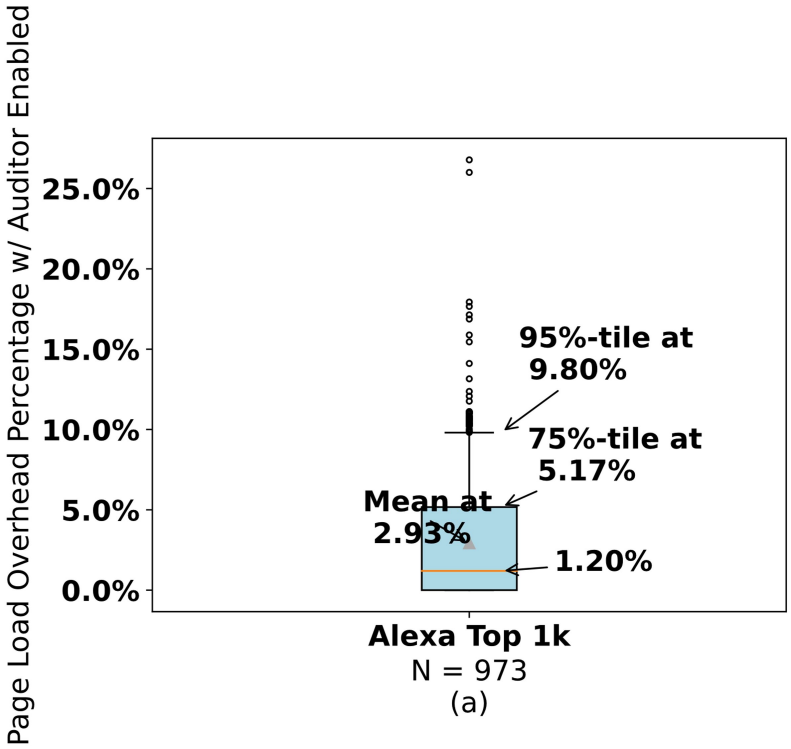
Evaluation: Runtime & Storage Overhead

Runtime Performance

- Page Load overhead of auditor was only 2.93% on average for Alexa 1k.
- Two outliers:
  - www.tripadvisor.com
  - www.atlassian.com

Storage Overhead

- 7.4 TB of disk space required per year for 1000 devices.



Conclusion

- Developed Mnemosyne, a postmortem watering hole forensic analysis engine.

- Evaluated Mnemosyne on 7 Attack Scenarios.
  - Mnemosyne was able to identify the victims in all scenarios.

- Mnemosyne reduces the analysis space by 98.17% and has only a 2.93% runtime overhead.

Questions?