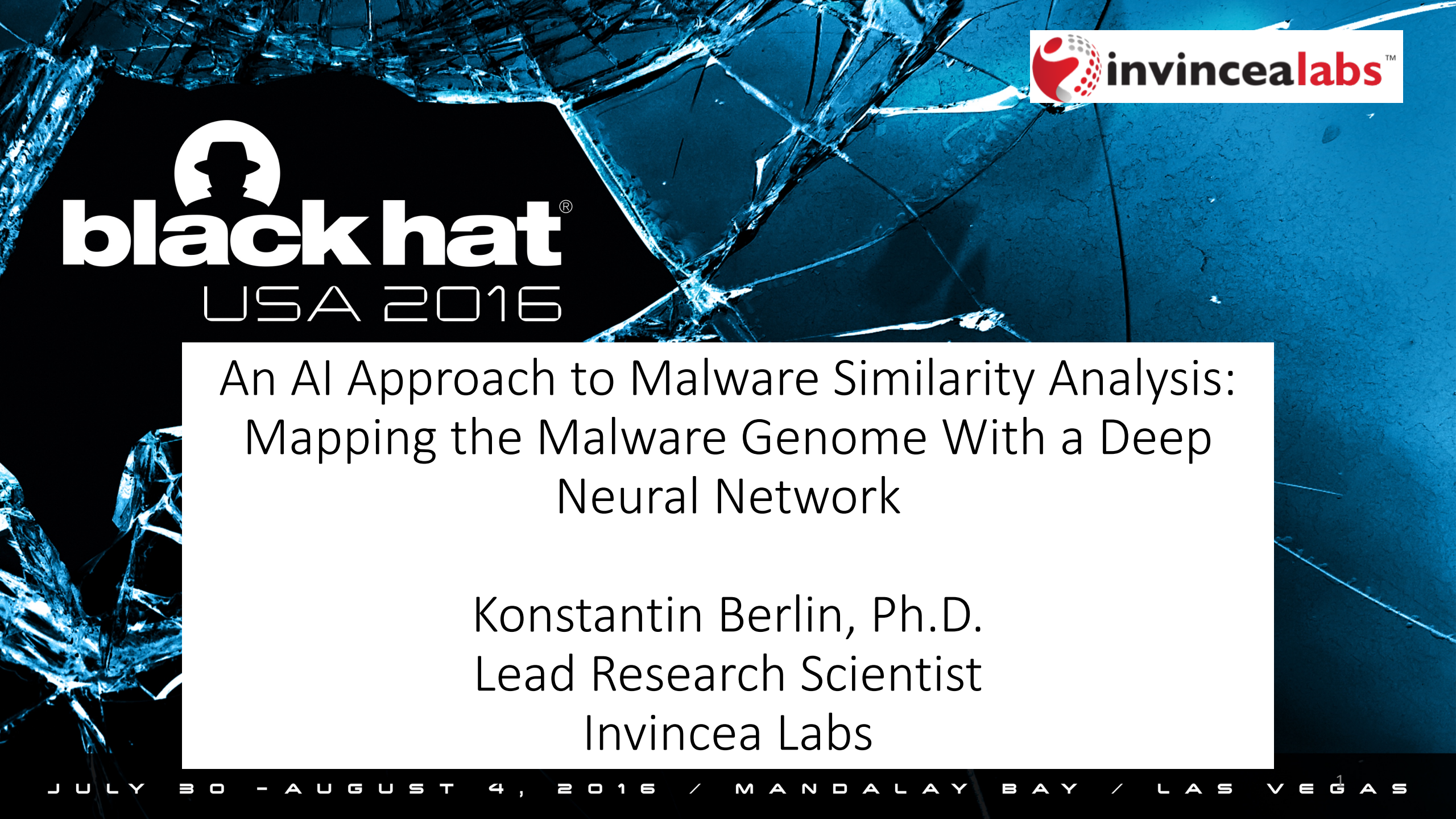


An AI Approach to Malware Similarity Analysis: Mapping the Malware Genome With a Deep Neural Network

Konstantin Berlin, Ph.D.
Lead Research Scientist
Invincea Labs

Why AI?

- Intelligence is critical for prevention and remediation
- AI is good at finding patterns in large data

Number of Network Breaches Per Year
(Verizon's 2016 Data Breach Investigations Report)

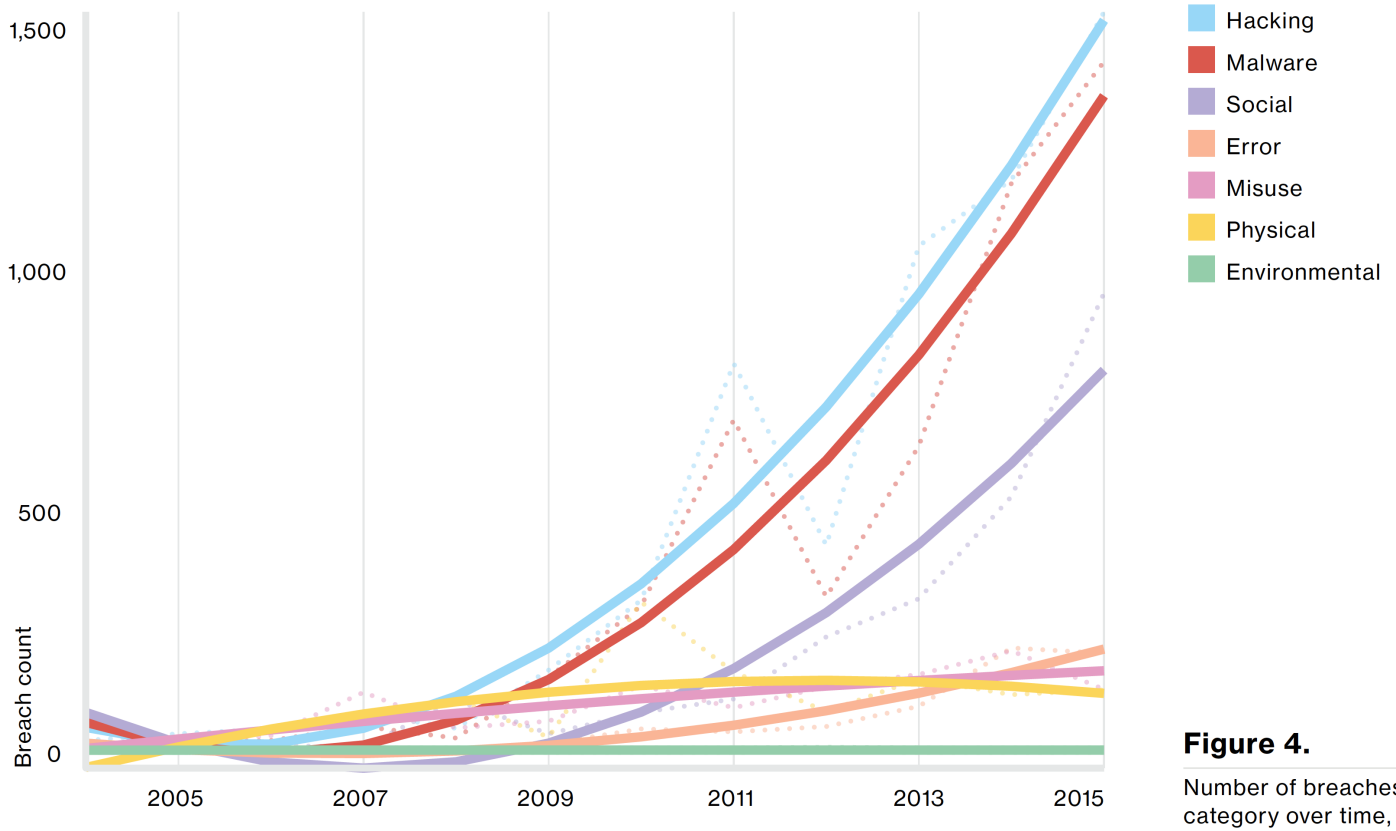
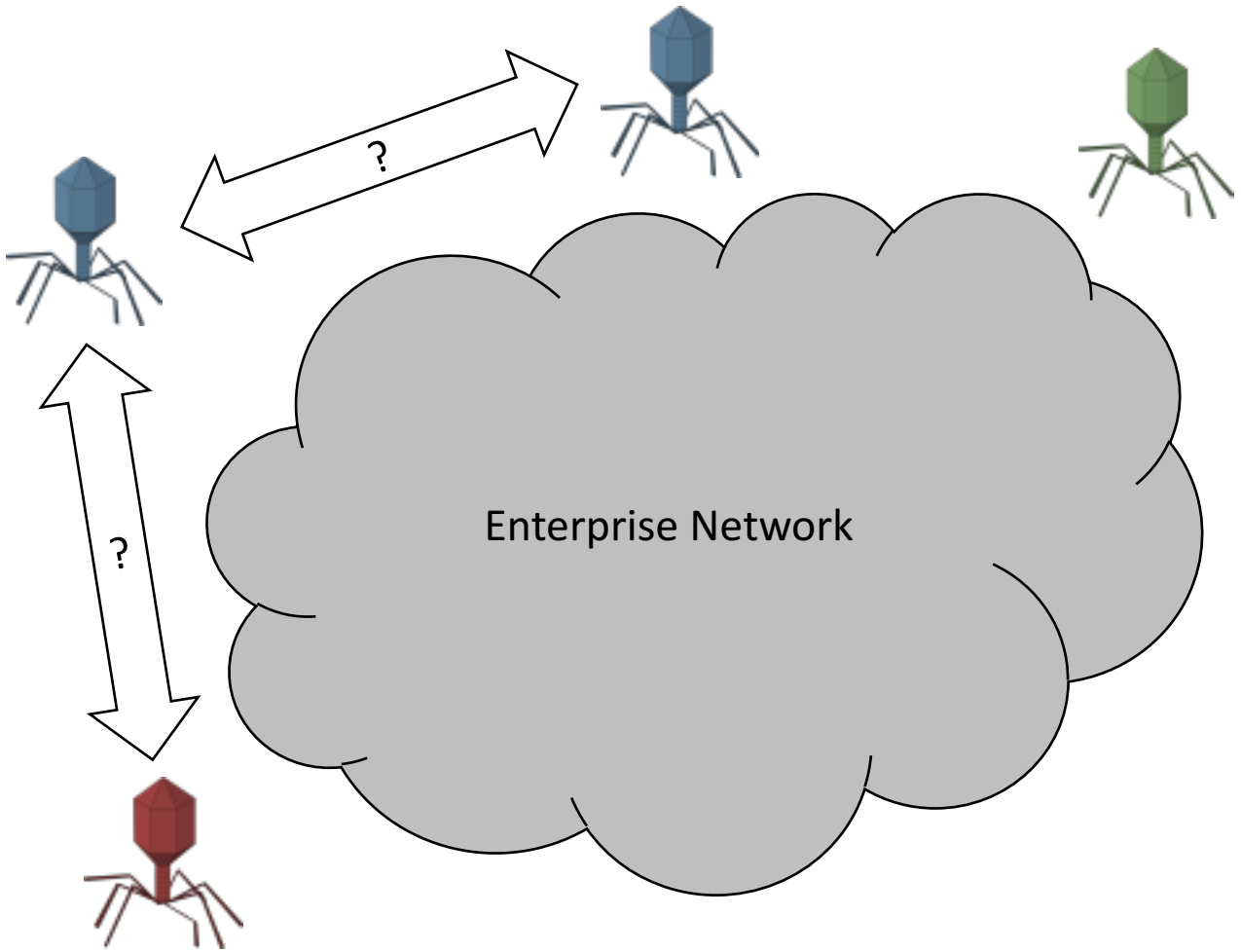


Figure 4.

Number of breaches per threat action category over time, (n=9,009)

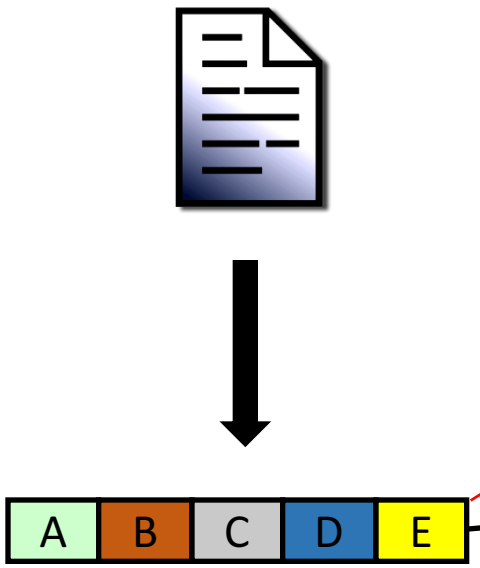
Intelligence through Similarity



- Benefits
  - Identify threat actors
    - Link various attacks to a single actor
  - Quickly understand functionality
    - Speed up reverse engineering
  - Mitigation
    - Signatures
    - Network Rules

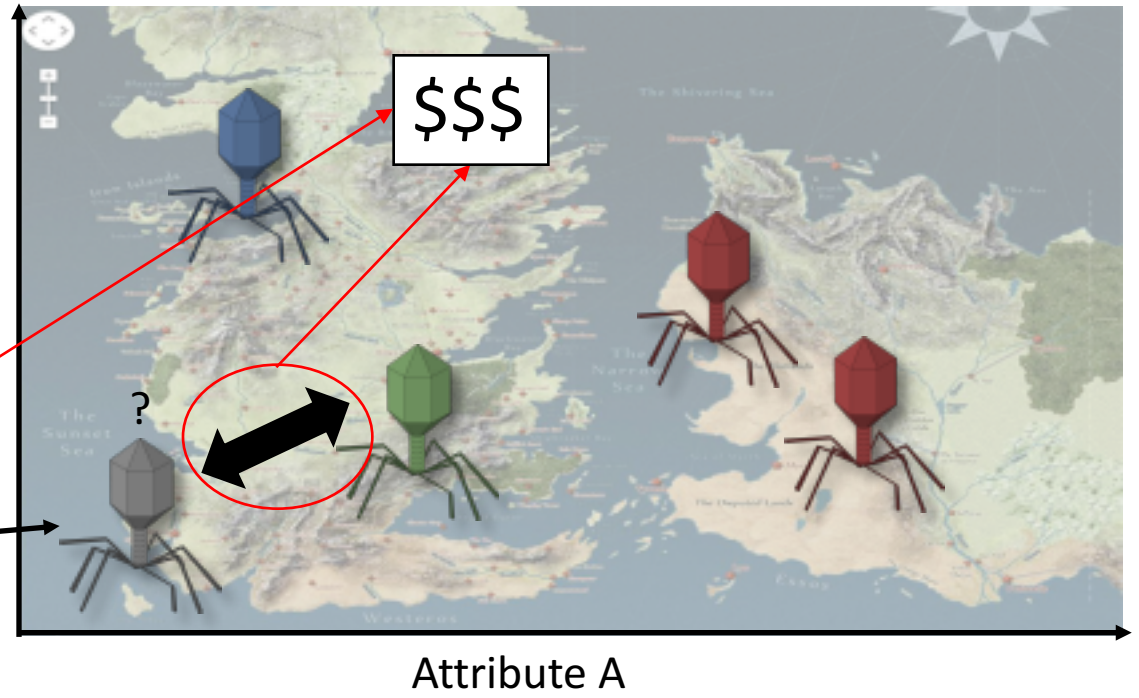
Finding Similar Malware

Attribute Extraction



Attributes
- Byte n-grams
- Opcode n-grams
- Printable strings
- System calls
- …

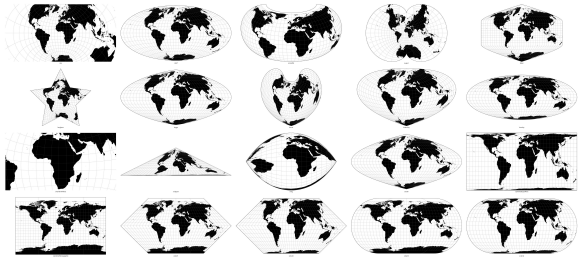
Attribute Map (**Embedding**)

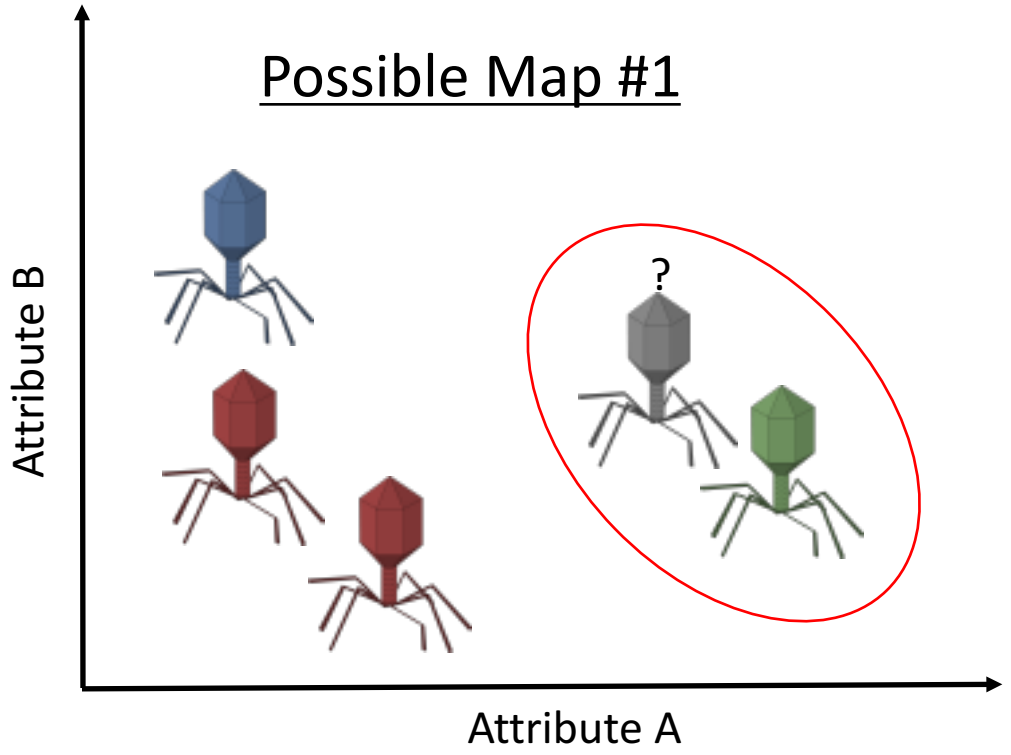


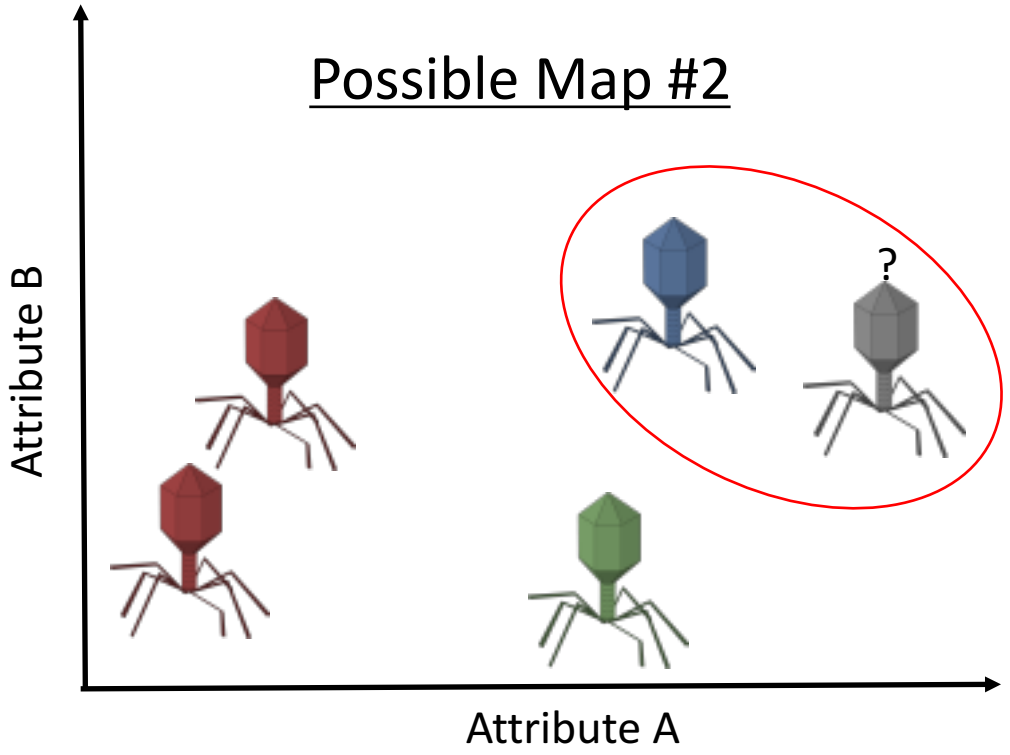
Similarity Search
- MinHash
- Feature hashing
- Other sketching
- …

Jang, Jiyong et. al. *Proceedings of the 18th ACM conference on Computer and communications security*. ACM, 2011.
Sæbjørnsen, Andreas, et al. *Proceedings of 18th international symposium on Software testing and analysis*. ACM, 2009.
Bayer, Ulrich, et al. *NDSS*. Vol. 9. 2009.
…Many more

Issues with Attribute Maps

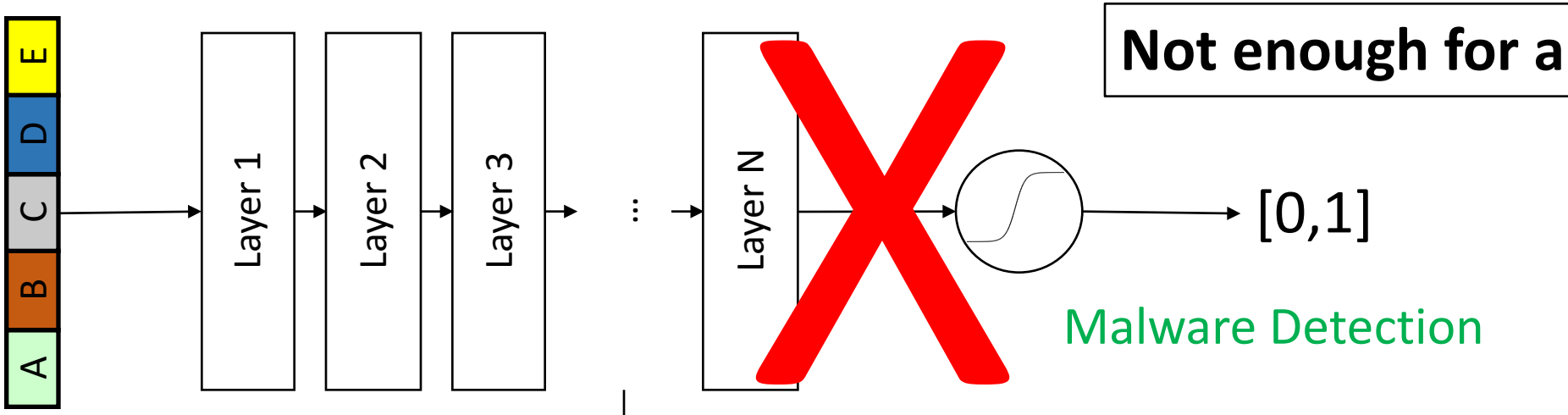






How to get consistent results, regardless of attributes?

Supervised Classification (Endpoint Solution)

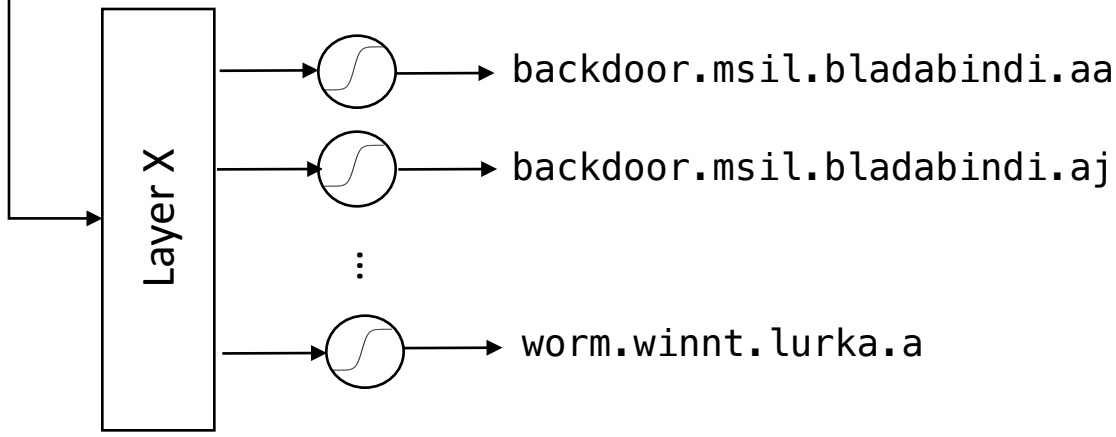


Not enough for a triage system!

Malware Detection

Joshua Saxe and Konstantin Berlin, *(MALWARE)*. IEEE, 2015.

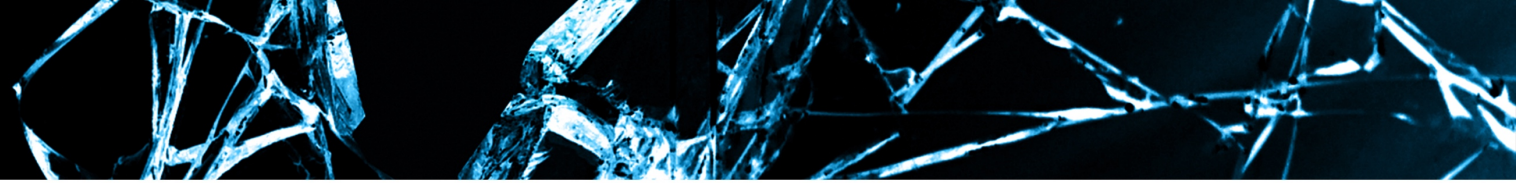
Categorical Classification



X by Invincea

0.97 F1-score (precision and recall)

- 1500 Microsoft Families
- 2.0M Training files



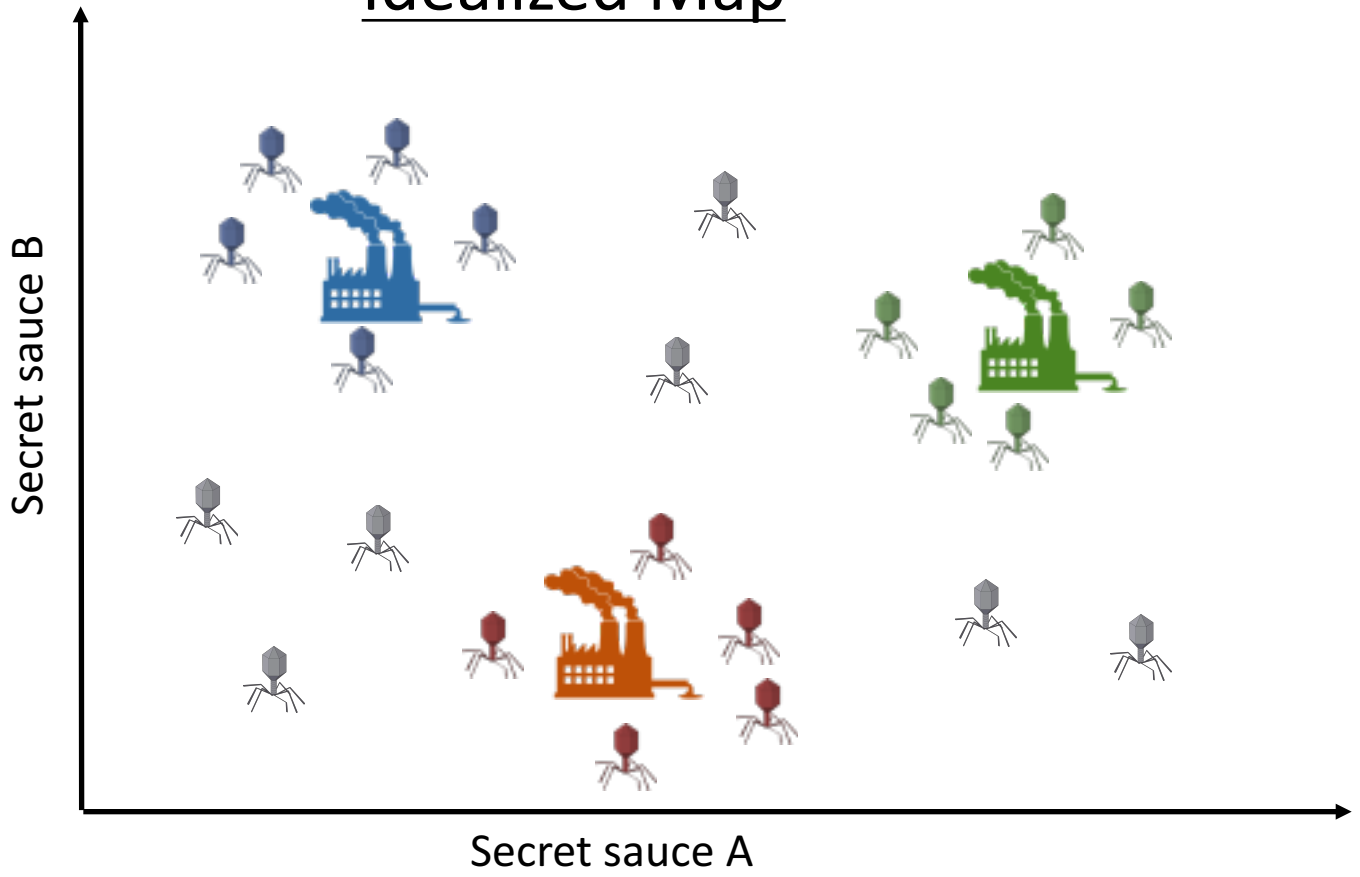
Given a set of attributes how do we create a “good” map?*

*No luck required

Imaginary World of Malware Factories

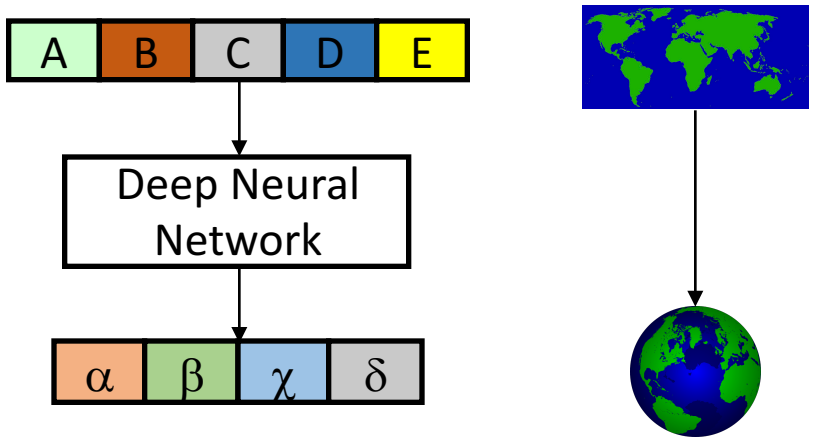
- Ideal World
  - Each hidden factory produces one malware family/variant
  - Factories are positioned relative to what and how they exploit vulnerabilities
- **…but this imaginary, no!?**

Idealized Map



There is No ~~Spoon~~ Map…

- We created the map when we selected the attributes
- We can morph them in any way we choose
- One good way to morph the attributes is using a deep neural network

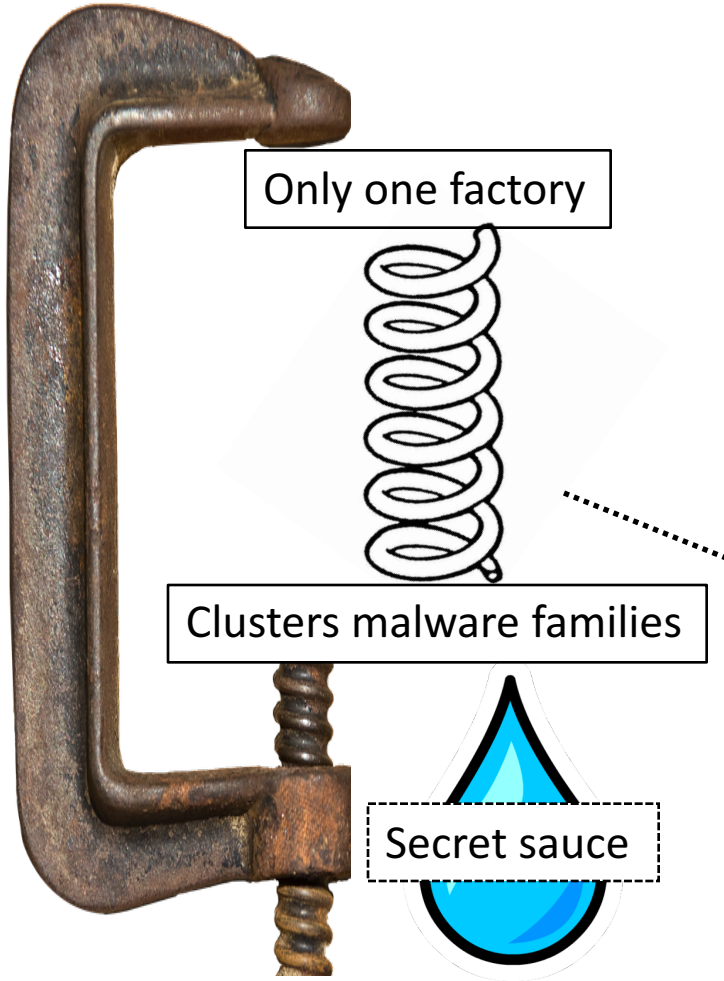


"The Matrix", 1999

Morphing the Map

Variational Autoencoder

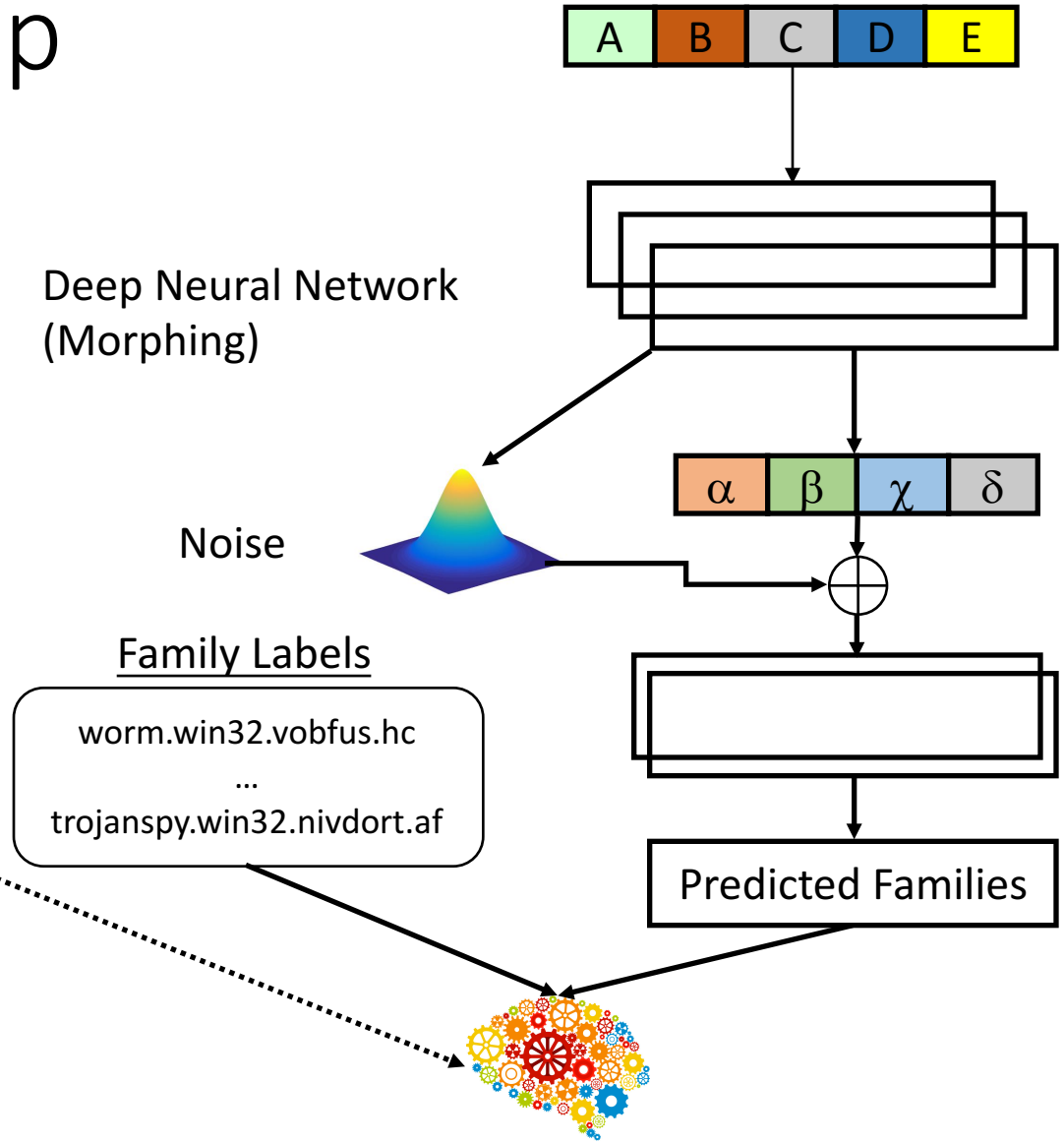
Kingma, D. P., & Welling, M. (2013). *arXiv preprint arXiv:1312.6114*.



Only one factory

Clusters malware families

Secret sauce



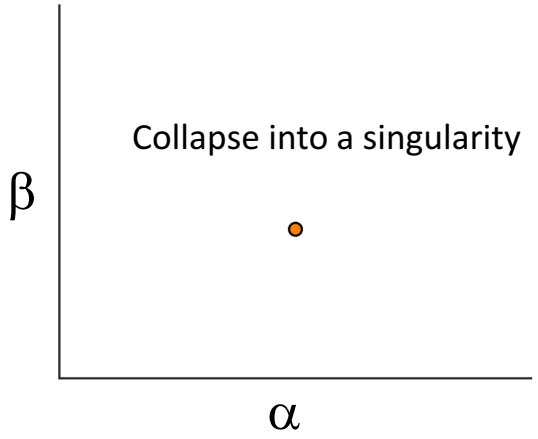
Toy Embedding Visualization

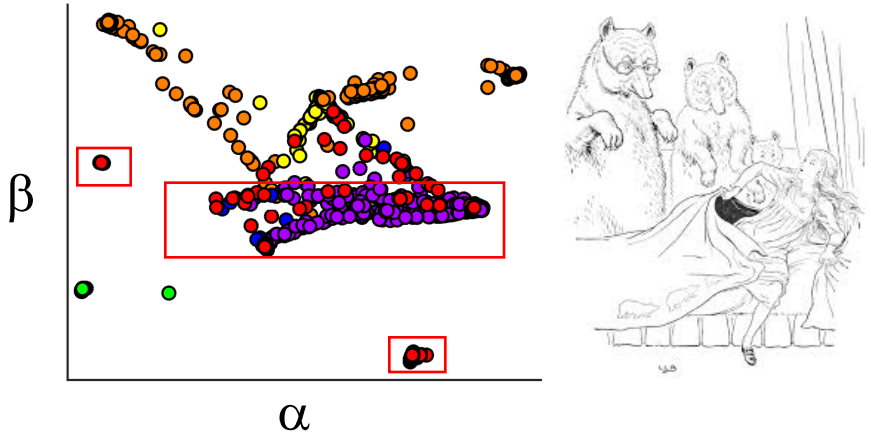
- Example
  - 8 family/variant prediction
  - 2D embedding

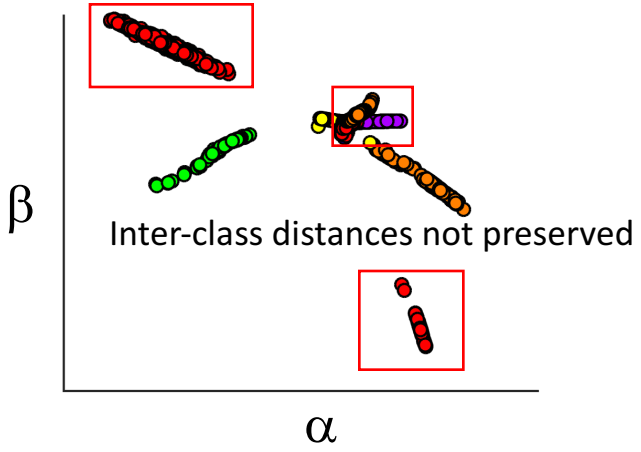
virus.win32.nabucur.d
virus.win32.ramnit.i
virus.win32.sality.at
virus.win32.shodi.i
virus.win32.virut.ae
virus.win32.virut.br
virus.win32.virut.k
worm.win32.allaple.a

Only one factory

Clusters malware families

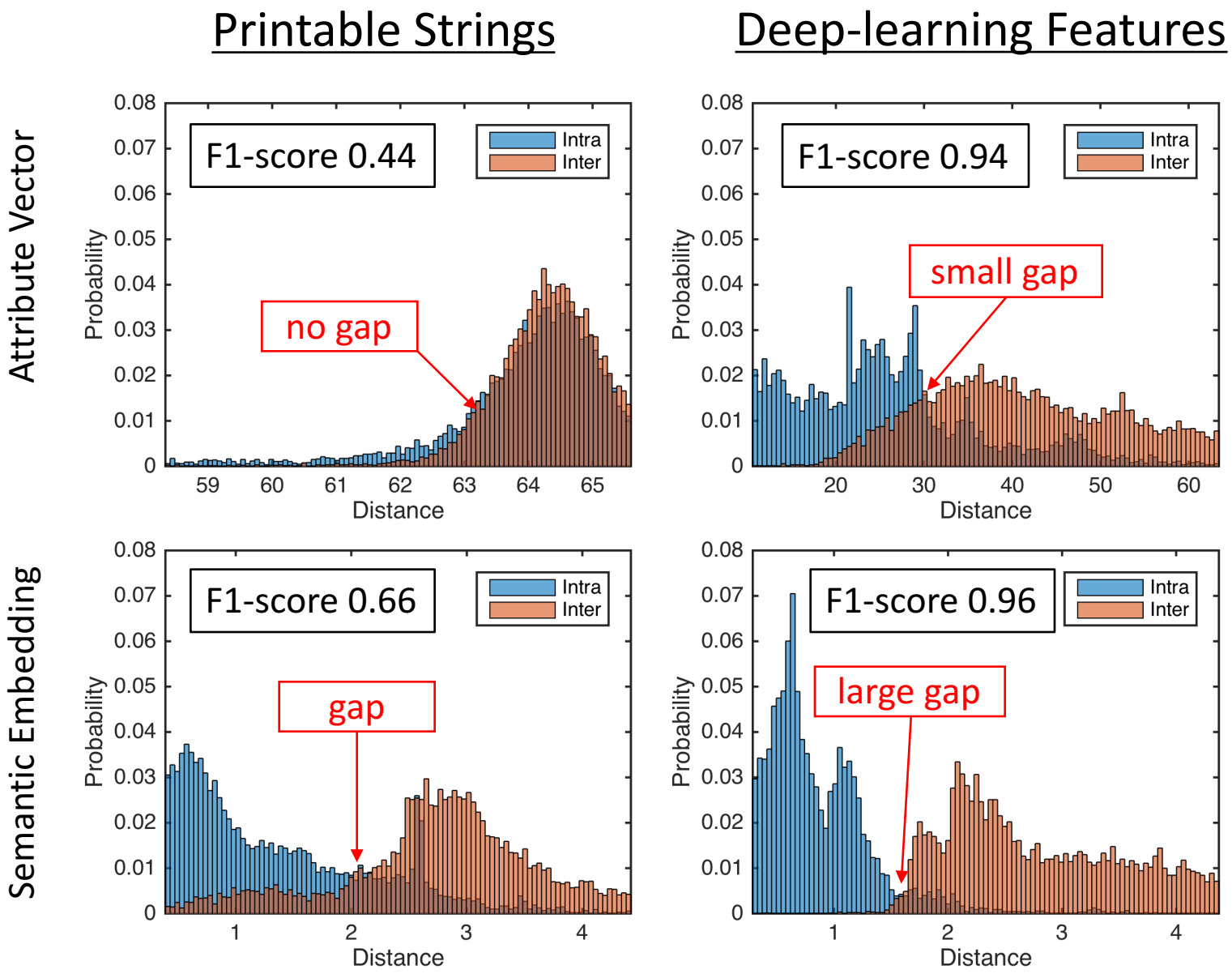






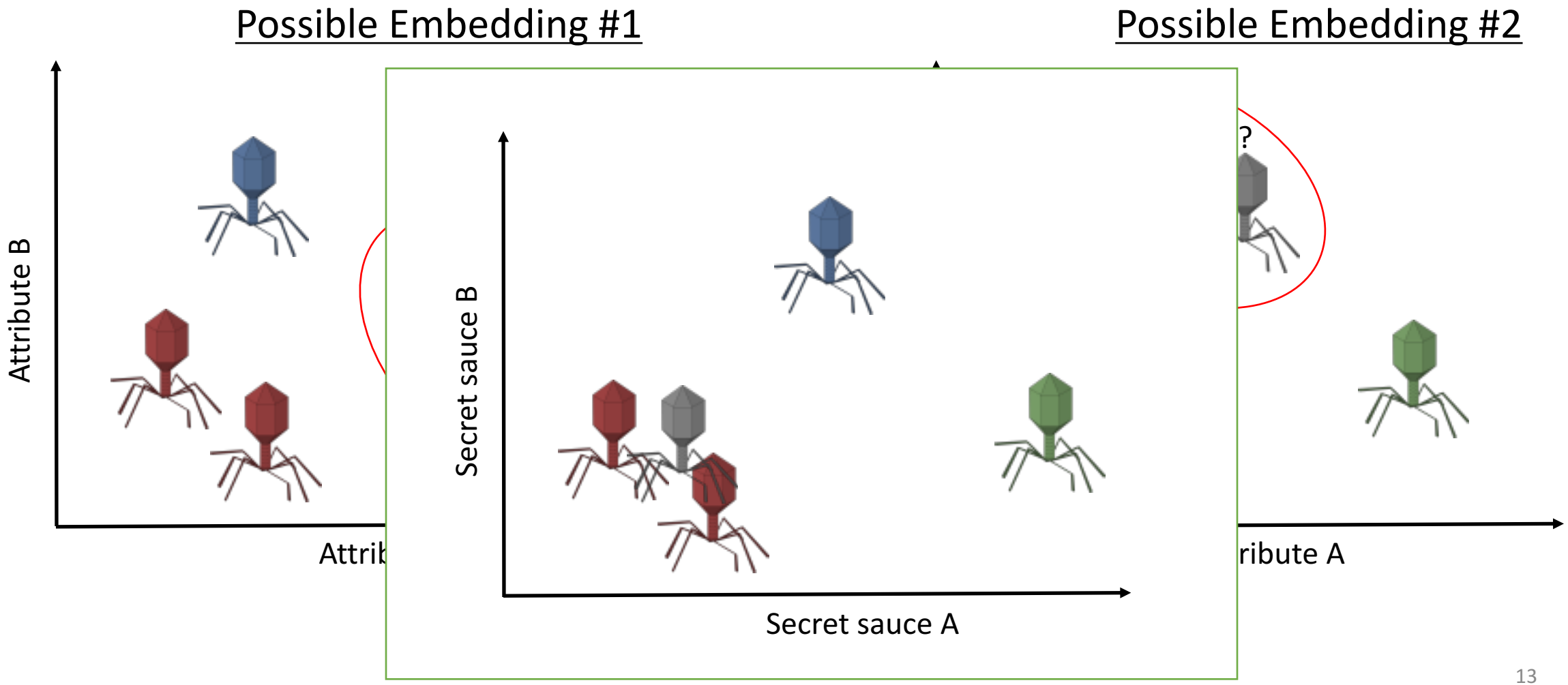
Results

- 800K samples
  - 1500 family/variants (99% coverage)
- Time-split Validation
  - Train on old data
  - Test on 30 days later
- Measure F1-score of 3-nearest neighbor classifier



Joshua Saxe and Konstantin Berlin, *(MALWARE)*. IEEE, 2015.

Issues with Attribute Maps



Conclusion

- Developing feature extraction is expensive and requires time consuming tuning to adapt to a specific domain
- Traditional approaches to malware similarity are hard to tune
- Using supervised-learning approaches we can improve existing features by embedding them into better maps
- **Automatic (re)tuning will improve attribution and reduce cost**

More Information

- Acknowledgement
  - Josh Saxe and Robert Gove
  - Invincea Inc.
- More information
  - Name: Konstantin Berlin
  - Email: kberlin@invincea.com
  - Twitter: @kberlin
- We are hiring!
  - Research Scientist
  - Senior Research Scientist
  - Principal Research Scientists

invincealabs™