Describing Malware via Tagging

Felipe N. Ducau

In collaboration with:

Ethan M. Rudd, Alex Long, Tad Heppner, Konstantin Berlin

SOPHOS

Malware Detection

- We already know that ML can be very powerful to detect malicious software.
  - Malicious / Benign, Confidence score

Malware Detection

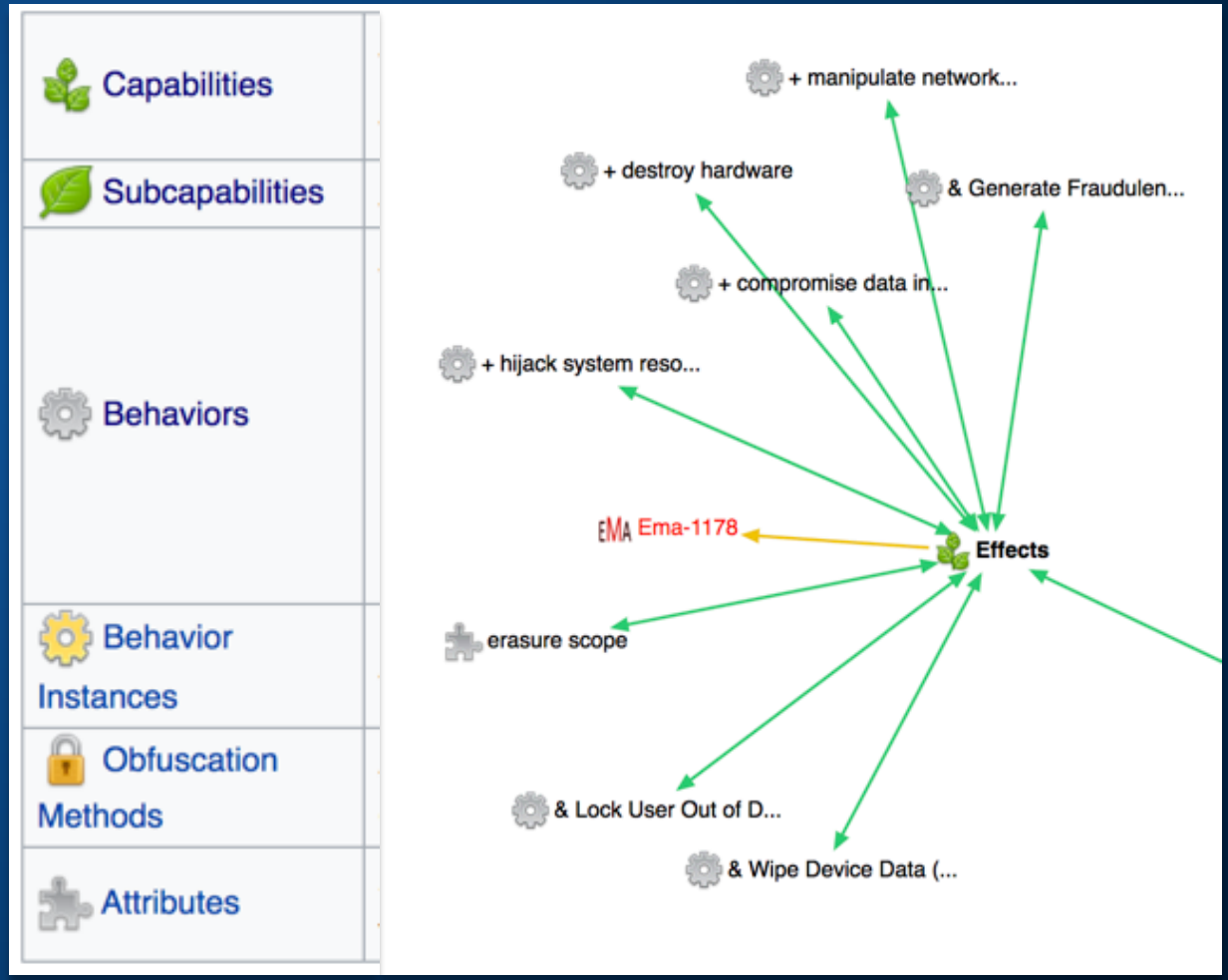
- We already know that ML can be very powerful to detect malicious software.
  - Malicious / Benign, Confidence score

Malware Description

- Can we **also** use it to describe the type of malware it detected?

Malware description: MAEC

- **Structured language** for encoding **high-fidelity** information about malware based on:
  - Behaviors
  - Artifacts
  - Relationships between samples



Malware description: Families

- Trojan-FNET!CCD9055108A1
- Win32.Virlock.Gen.8
- W32.Virlock!inf7
- TR/Crypt.ZPACK.Gen
- Trojan (004d48ee1)
- Virus:Win32/Nabucur.D
- W32/VirRnsm-F
- Virus.Win32.PolyRansom.k
- W32/Virlock.J
- a variant of Win32/Virlock.J

Malware description: Families

- Trojan-FNET!CCD9055108A1
- Win32.Virlock.Gen.8
- W32.Virlock!inf7
- TR/Crypt.ZPACK.Gen
- Trojan (004d48ee1)
- Virus:Win32/Nabucur.D
- W32/VirRnsm-F
- Virus.Win32.PolyRansom.k
- W32/Virlock.J
- a variant of Win32/Virlock.J

virlock virlock nabucur rnsm, ransom polyransom virlock virlock

(ransomware)

Malware description: Families

- Trojan-FNET!CCD9055108A1
- Win32.Virlock.Gen.8
- W32.Virlock!inf7
- TR/Crypt.ZPACK.Gen
- Trojan (004d48ee1)
- Virus:Win32/Nabucur.D
- W32/VirRnsm-F
- Virus.Win32.PolyRansom.k
- W32/Virlock.J
- a variant of Win32/Virlock.J

virlock virlock nabucur rnsm, ransom polyransom virlock virlock

(ransomware)

virrnsm

(file-infector)

Malware description: Families

- Trojan-FNET!CCD9055108A1
- Win32.Virlock.Gen.8
- W32.Virlock!inf7
- TR/Crypt.ZPACK.Gen
- Trojan (004d48ee1)
- Virus:Win32/Nabucur.D
- W32/VirRnsm-F
- Virus.Win32.PolyRansom.k
- W32/Virlock.J
- a variant of Win32/Virlock.J

virlock virlock nabucur rnsm, ransom polyransom virlock virlock

(ransomware)

virrnsm

(file-infector)

crypt zpack

(packed)

Tags from Tokens

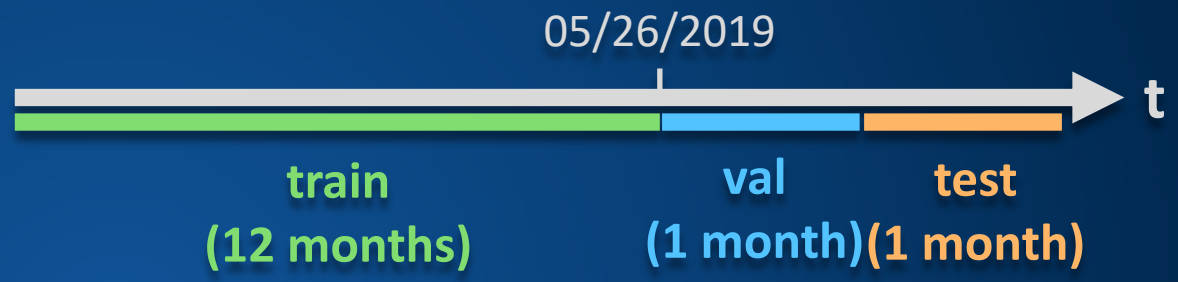
Detection name	Tokens	Tags
Artemis!4A26E203524C, Downloader, a variant of Win32/Adware.Adposhel.AM.gen, None, None, None, Gen:Variant.Razy.260309, None, Trojan (005153df1), Riskware/Adposhel	artemis, downloader, variant, win32, adware, adposhel, gen, gen, variant, razy, trojan, riskware, adposhel	adware downloader
W32.Virlock!inf7, TR/Crypt.ZPACK.Gen, Trojan (004d48ee1), Virus:Win32/Nabucur.D, W32/VirRnsm-F, Virus.Win32.PolyRansom.k, Win32.Virlock.Gen.8, W32/Virlock.J, Trojan-FNET!CCD9055108A1, a variant of Win32/Virlock.J	w32, virlock, inf7, tr, crypt, zpack, gen, trojan, win32, nabucur, w32, vir, rnsm, virrnsm, win32, poly, ransom, polyransom, win32, virlock, gen, trojan, variant, win32, virlock	ransomware packed file-infector

Dataset Creation

- **Only malware samples** 
- **Train set**
  - M: 10,000,000
  - XL: 76,205,000
- **Val set**
  - 3,159,377
- **Test set**
  - 3,784,746

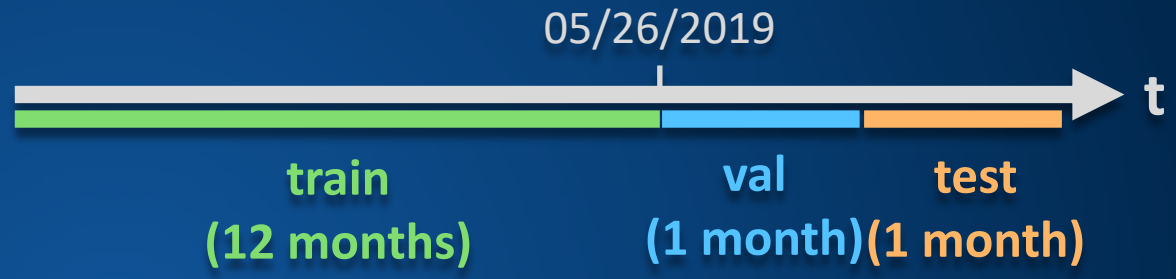
Dataset Creation

- **Only malware samples**
- **Train set**
  - M: 10,000,000
  - XL: 76,205,000
- **Val set**
  - 3,159,377
- **Test set**
  - 3,784,746



Dataset Creation

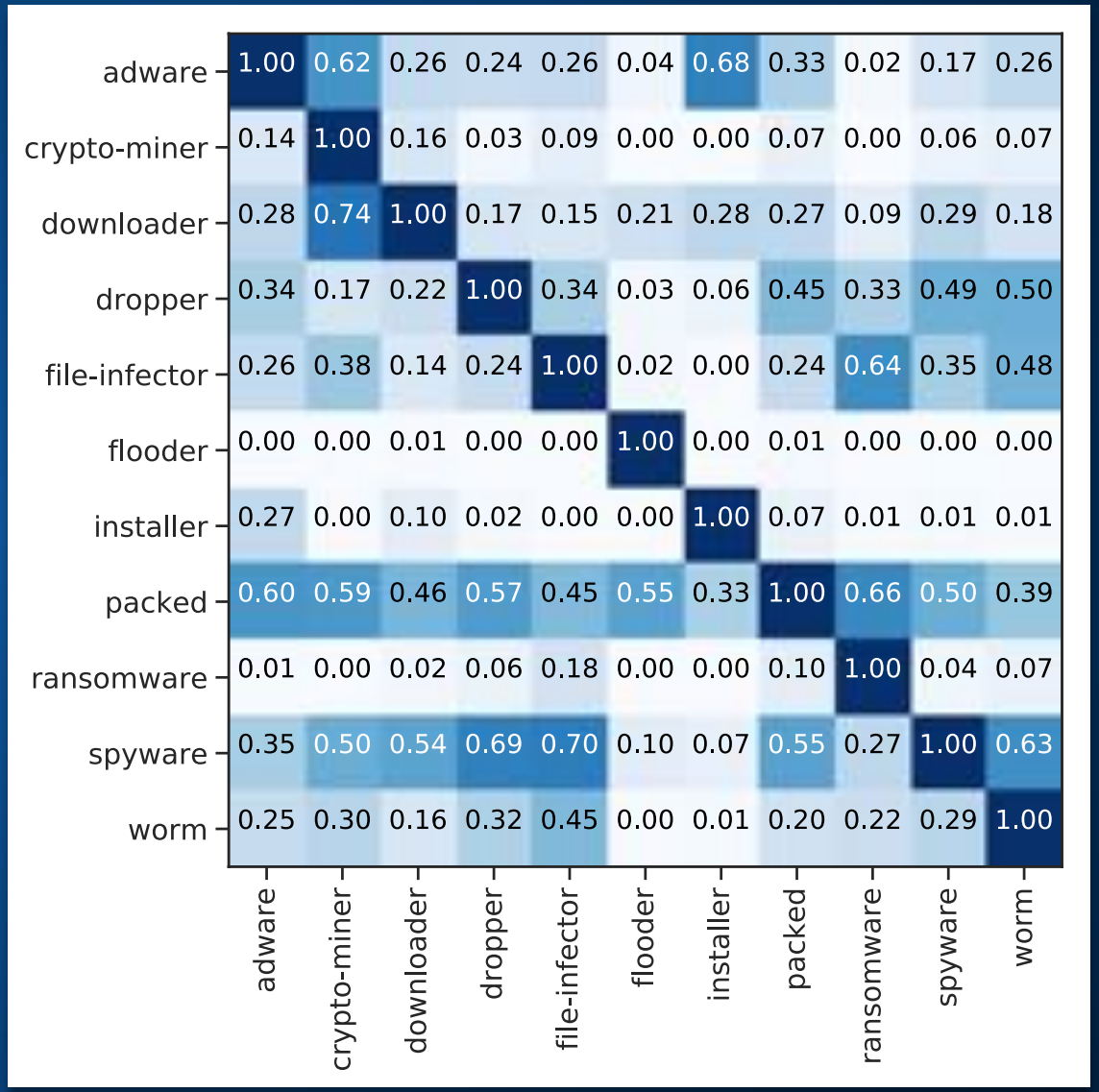
- **Only malware samples** 
- **Train set**
  - **M**: 10,000,000
  - **XL**: 76,205,000
- **Val set**
  - 3,159,377
- **Test set**
  - 3,784,746



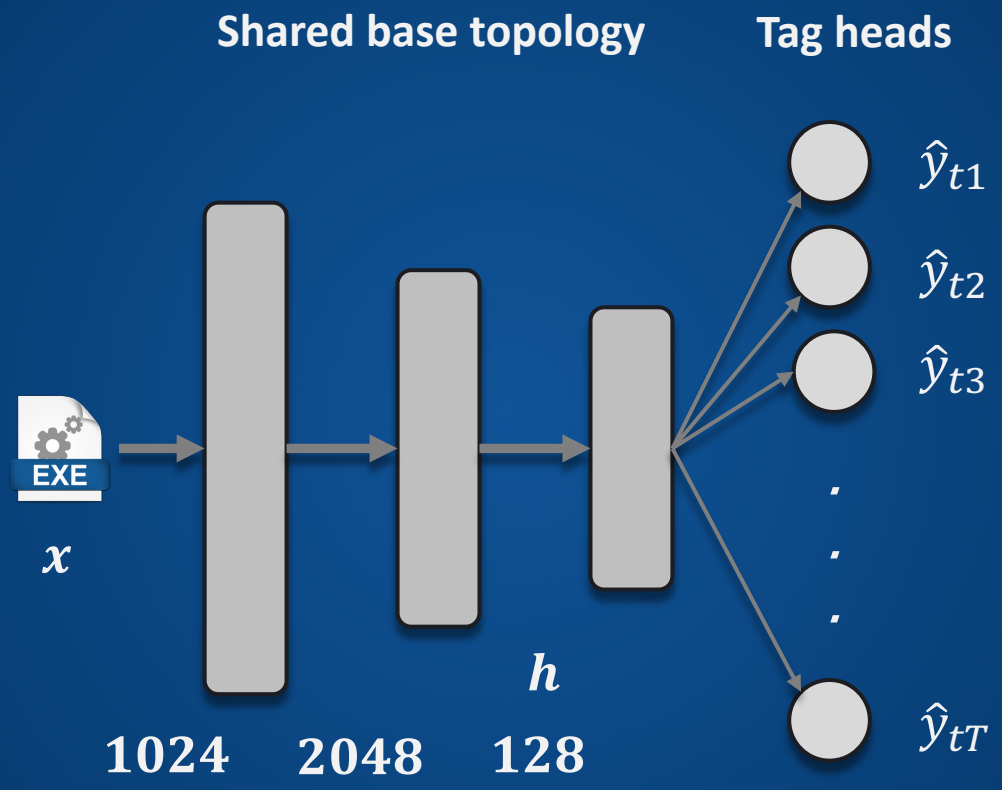
- 2D binary entropy **features** as in Saxe & Berlin, 2015.
- **Labels** from data-driven augmentation of token-to-tag mapping.

Tags distribution

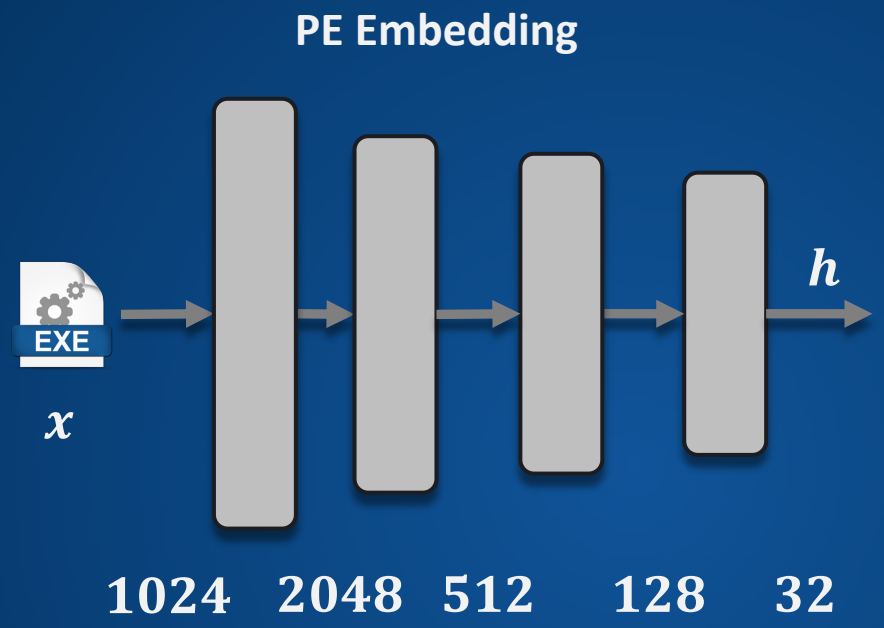
- **packed** 30.31%
- **spyware** 29.96%
- **dropper** 24.04%
- **worm** 20.63%
- **file-infector** 20.23%
- **downloader** 17.86%
- **adware** 16.95%
- **installer** 8.56%
- **ransomware** 8.13%
- **crypto-miner** 2.28%
- **flooder** 0.79%



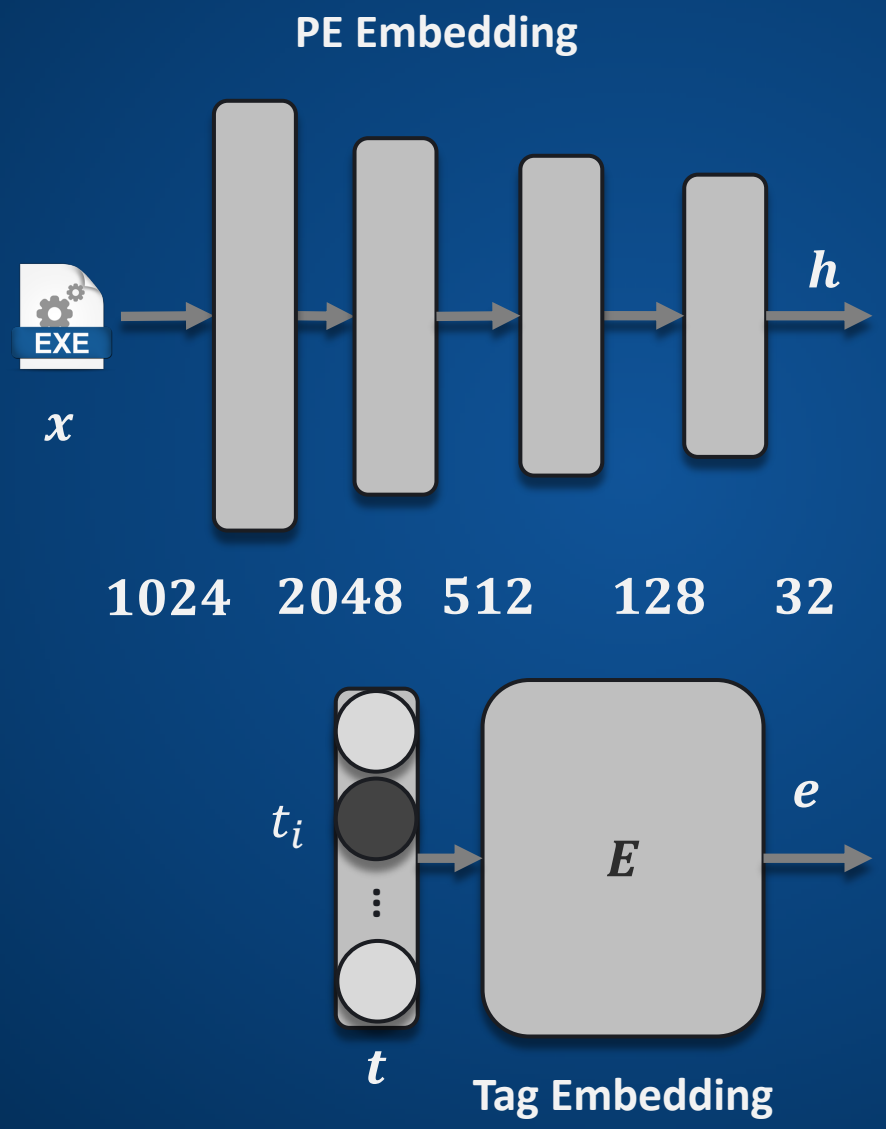
Model 1: Multi-head



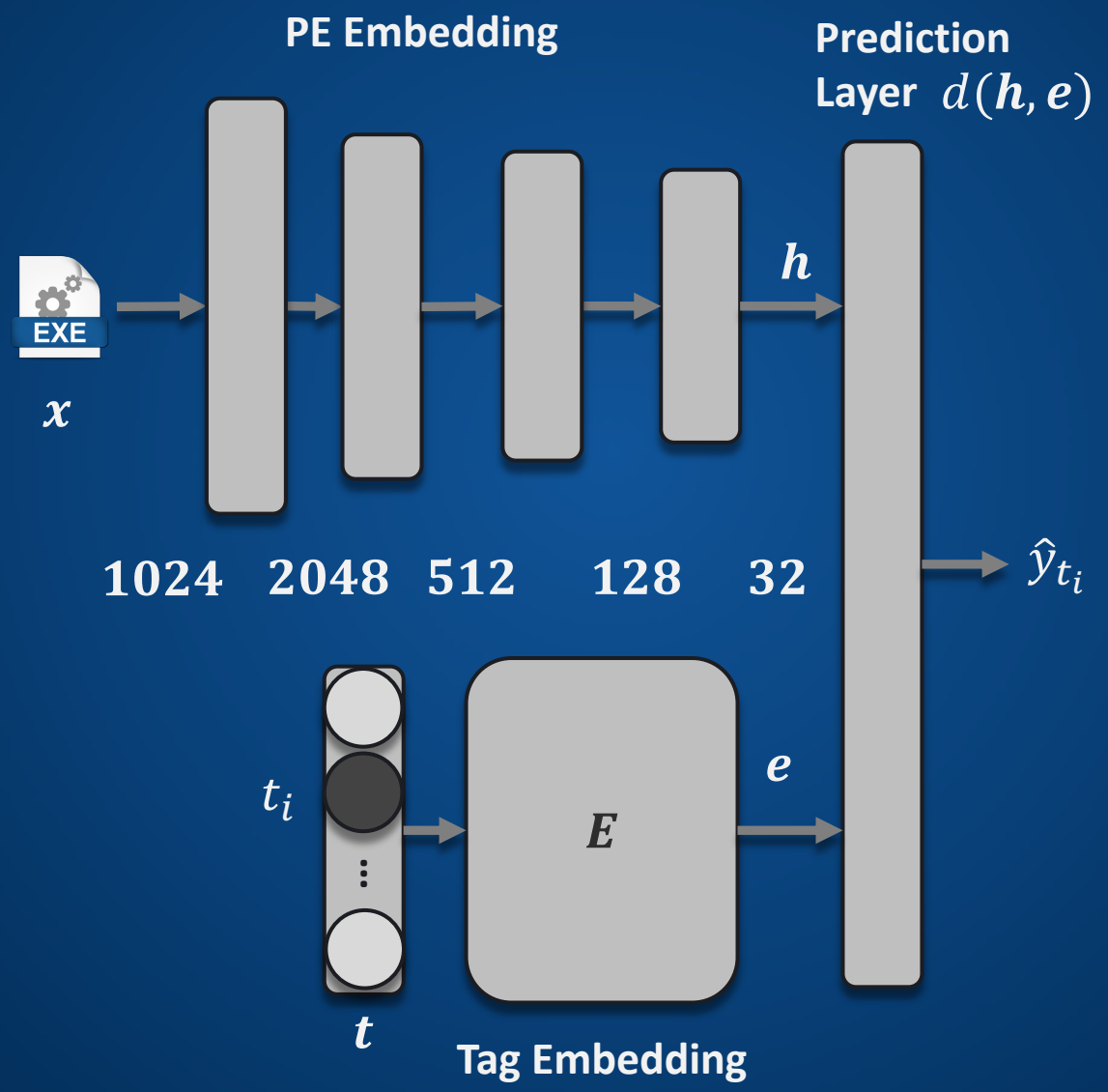
Model 2: Joint Embedding



Model 2: Joint Embedding



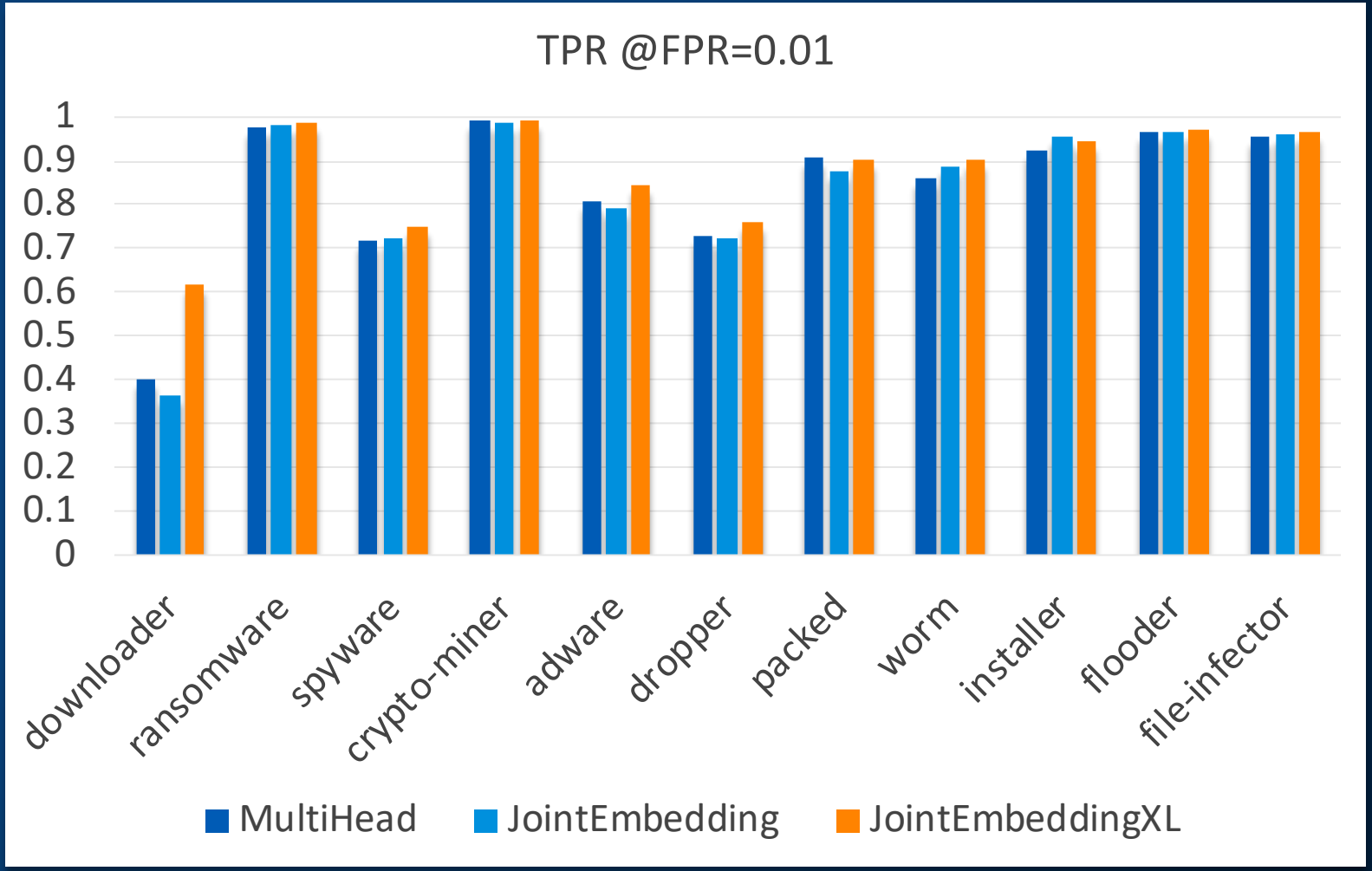
Model 2: Joint Embedding



Evaluation: Per Tag

- **JointEmbedding XL**
  - **Mean TPR:** 0.88
  - **Mean AUC:** 0.99

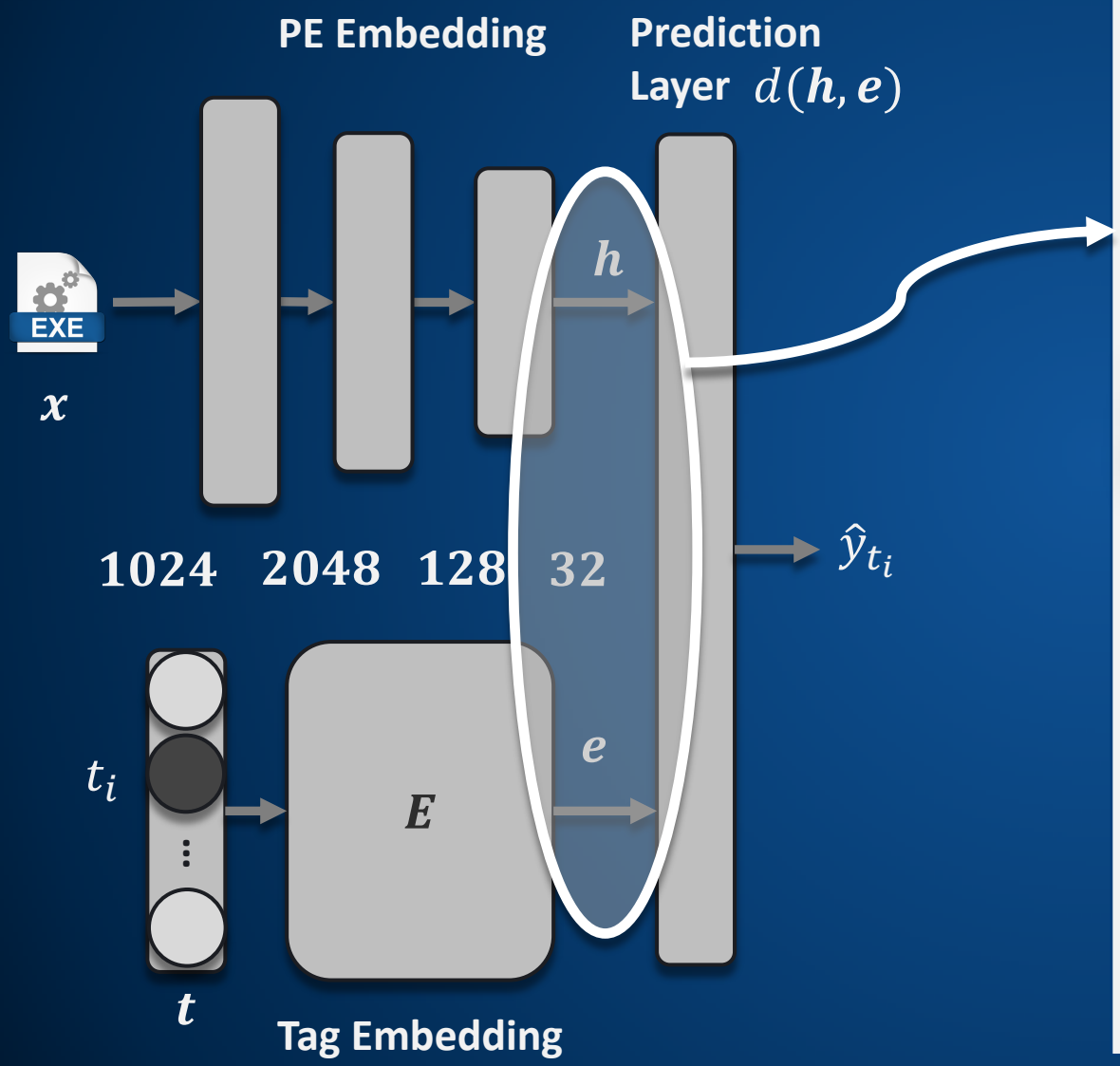
- 71% of the files for which **all** the tags are correctly predicted.

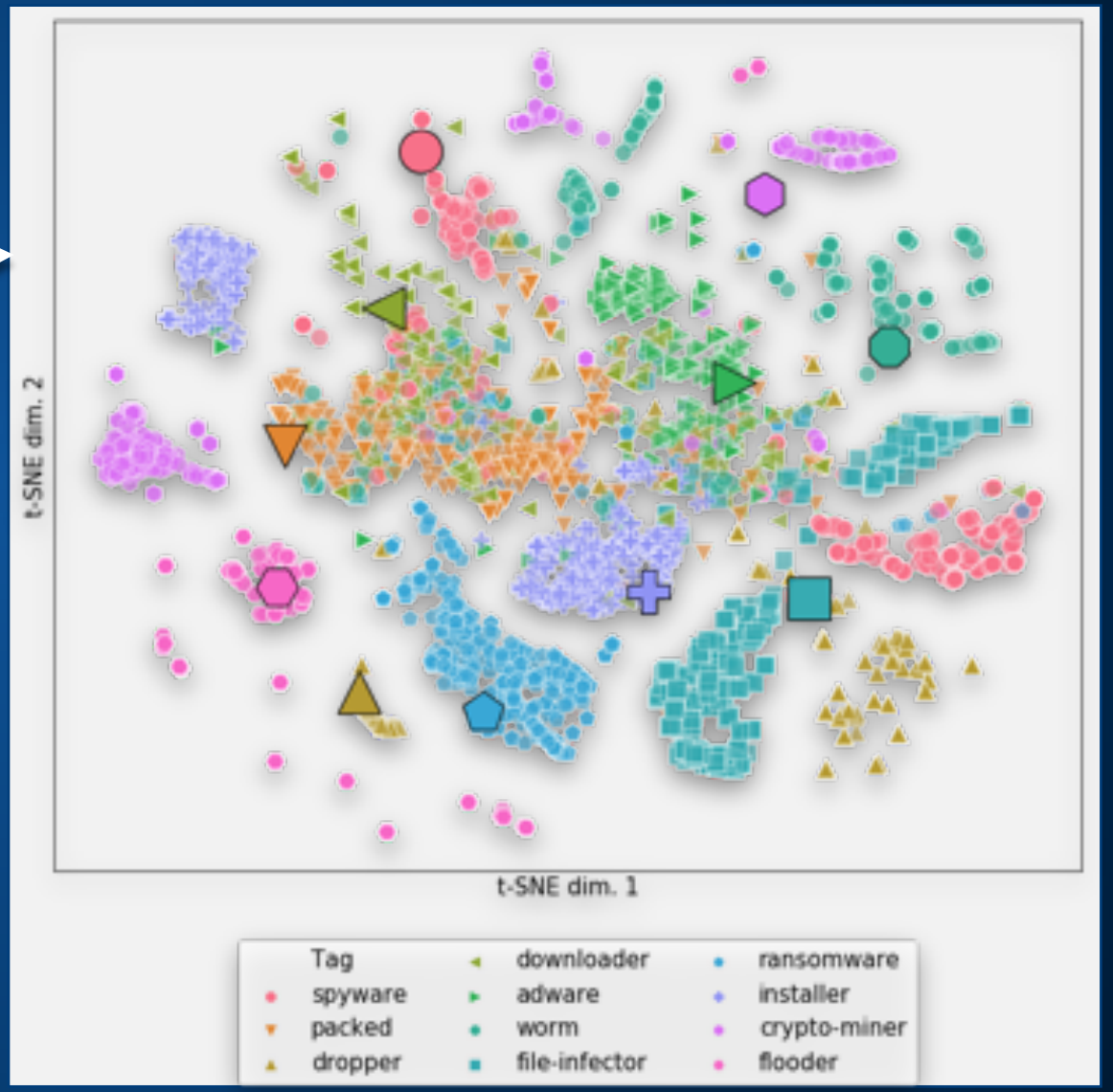


Tagging : Use-cases

- Generate contextual information.
  - Provide to consumers
  - Use internally
- Ability of **prioritize** and **cluster** events based on threat characteristics.
- Common “light-weight” description framework.
  - Can be extended to various detection/analysis technologies.
- Improve standard Malware/Benign classification
  - **ALOHA: Auxiliary Loss Optimization for Hypothesis Augmentation**
    Ethan M. Rudd, Felipe N. Ducau, Cody Wild, Konstantin Berlin, and Richard Harang
    Usenix, 2019.

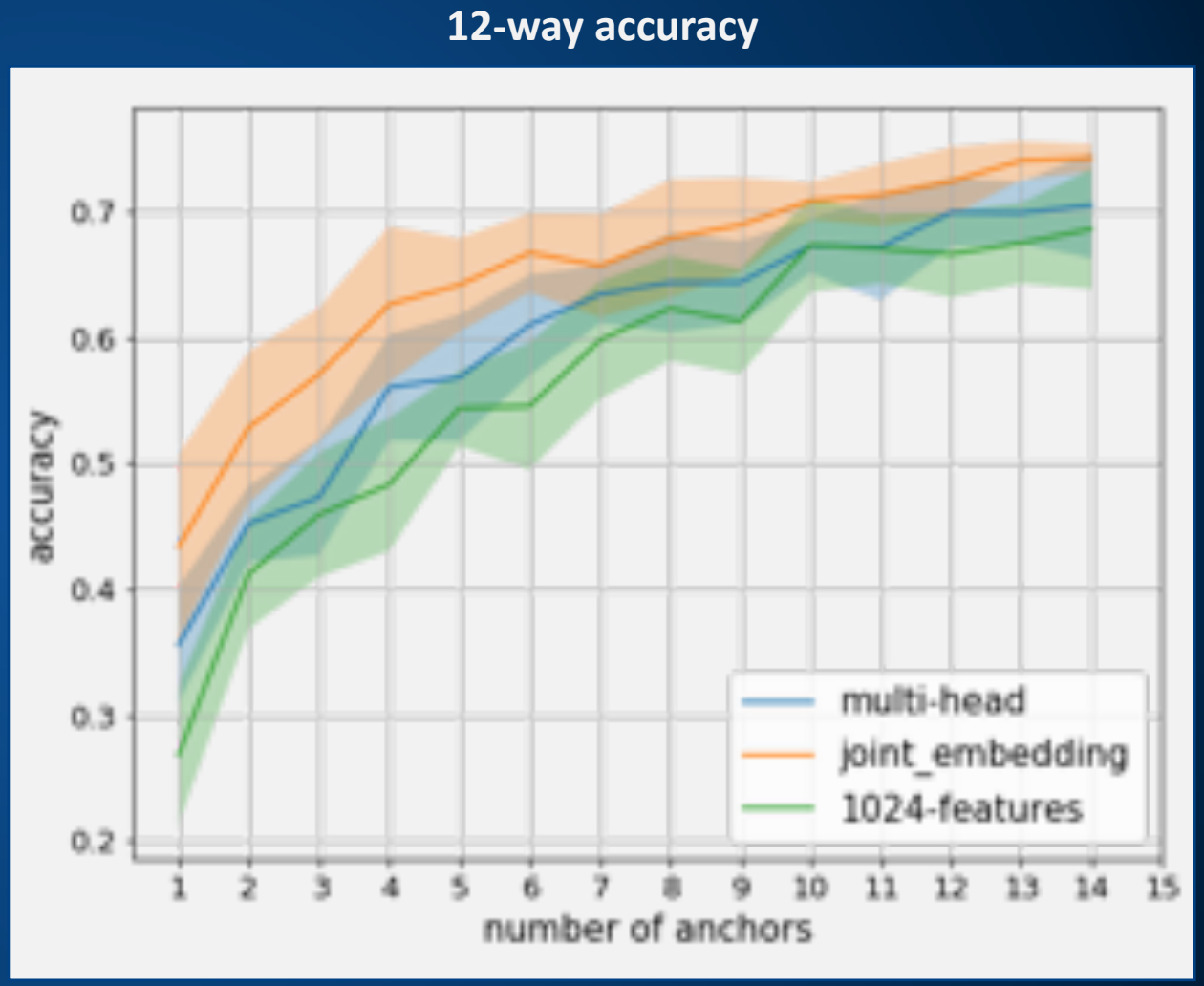
Joint embedding space
via t-sne





Joint embedding space
similarity index

- Select samples in test set for which we have a good knowledge about their families (~1,500).
  - upatre, bladabindi, nanocore, emotet, darkcomet, …
- Measure similarity between test samples and **anchor** test samples.
- Predict **family** based on closest anchor in embedding space.



That’s all folks!

SMART: Semantic Malware Attribute Relevance Tagging
Felipe N. Ducau, Ethan M. Rudd, Alex Long, Tad Heppner, Konstantin Berlin
2019 pre-print, arXiv:1905.06262

@fel_d
fducau.github.io

SOPHOS