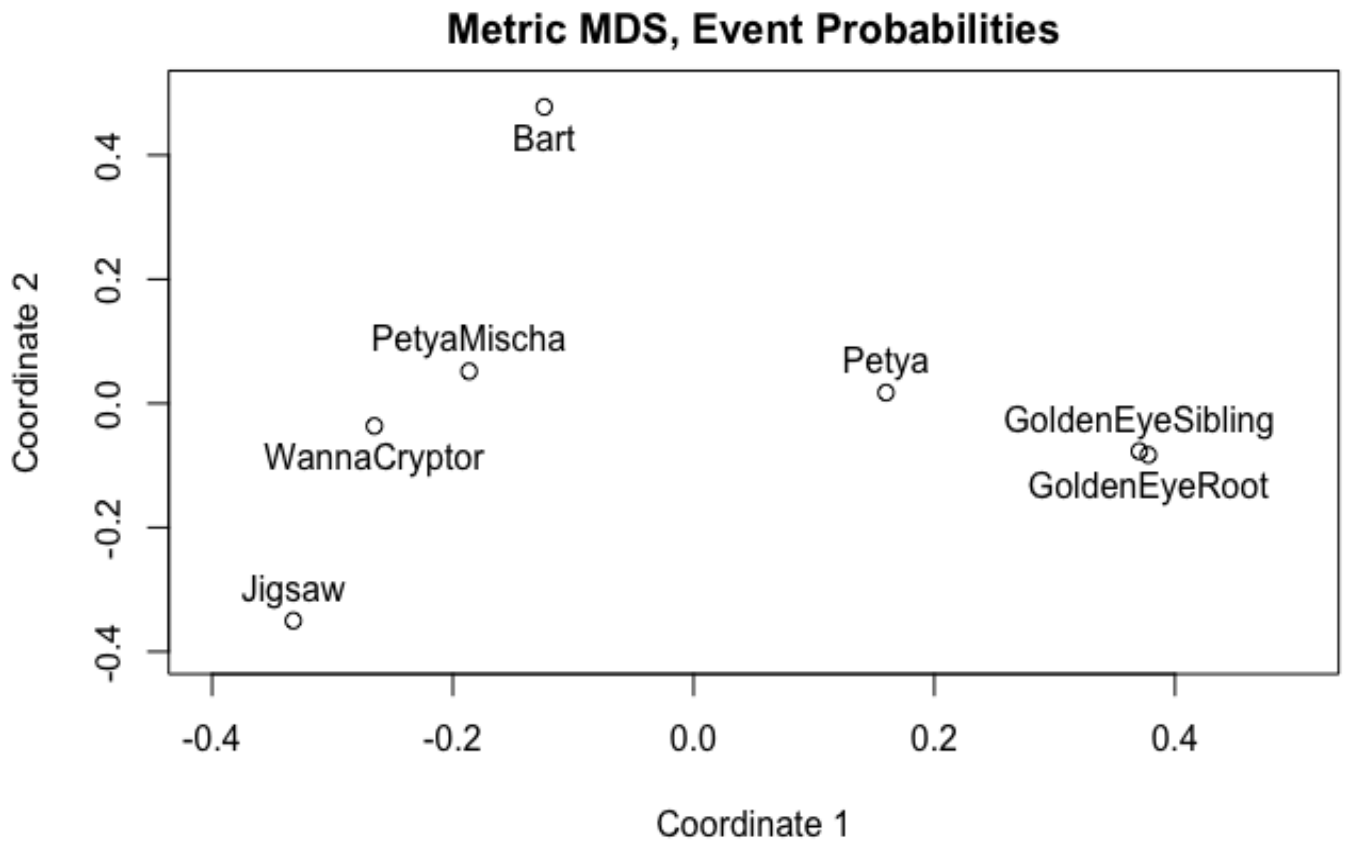
A Grammar-Based Behavioral Distance Measure among Ransomware Variants



H. Van Dyke Parunak, Ph.D.
van.parunak@gmail.com

H. V. D. Parunak. A Grammar-Based Behavioral Distance Measure Between Ransomware Variants. IEEE Transactions on Computational Social Systems, 9(1):8-17, **2022**.

12TH ANNUAL HOT TOPICS in the SCIENCE OF SECURITY
April 1 - 3, 2025 | VIRTUAL

Overview

- Key thesis
- Getting Data
- Formalizing the Model
- Applying the Model to the Data
- Next Steps

Key Thesis of RADAR (Ransomware Analysis as Dialog for Attribution and Reconnaissance)

"Facts are stupid things, until brought into connection with some general law." Louis Agassiz, Harvard University, ca. 1860.

1. Current methods of attribution are based on *isolated* characteristics of an attack (e.g., code signatures, distribution botnet).
2. Ransomware involves the victim in a *dialog* with the attacker.
3. This dialog can be characterized *linguistically* to identify organic patterns.
4. These patterns *integrate details* to help attribute attacks.

A Tale of Two (or more) Attacks…

Petya:

Pfishing Email → Fake Job Application → Rewrite MBR → Encrypt MFT → Custom Lock Display → Tor

Bart:

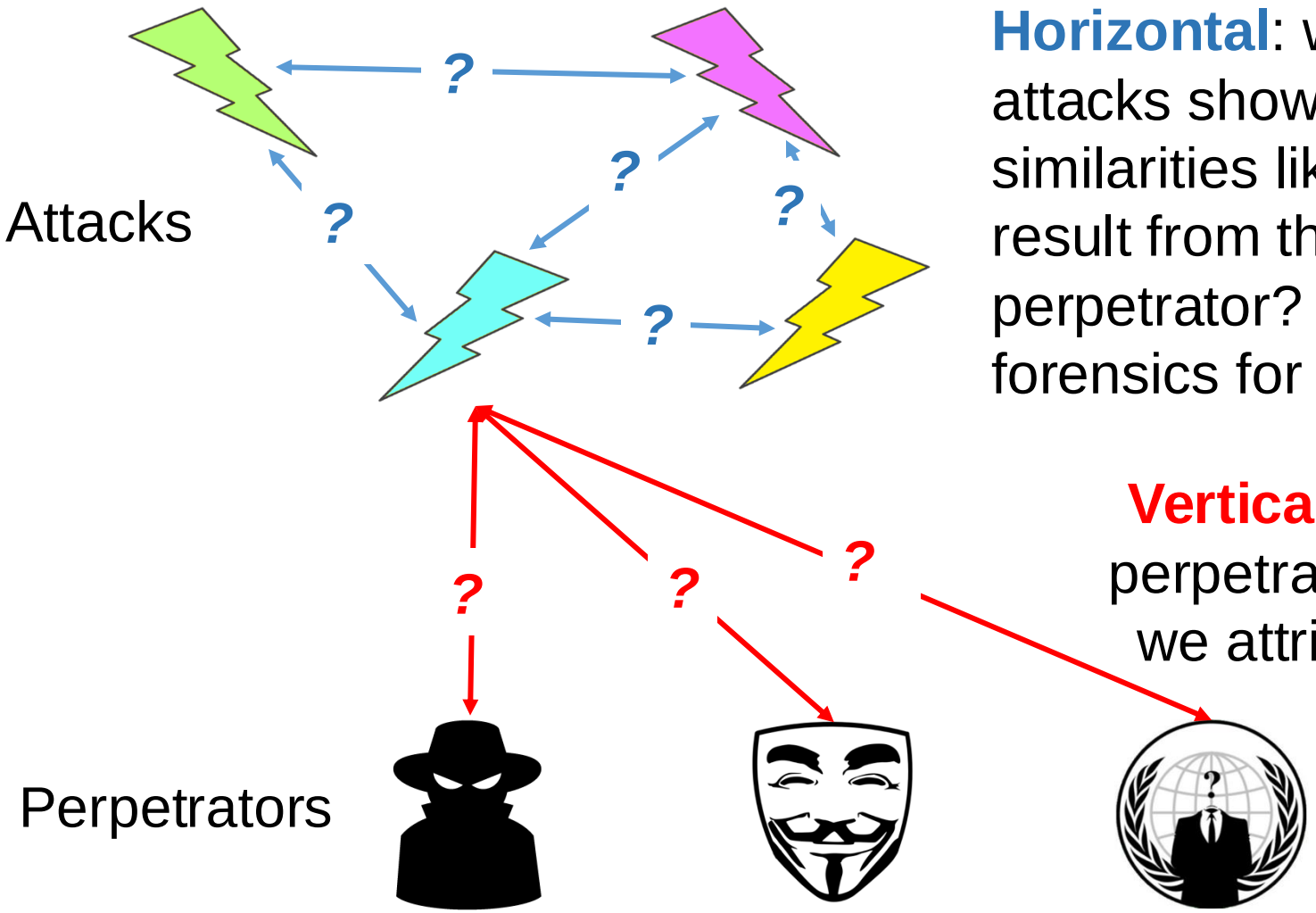
Necurs → ZIPFile → Rock Loader → zip Encryption → noticeIn Directories → Tor

GoldenEye:

Breach Update System → Auto Update → Eternal Blue → Rewrite MBR → Encrypt MFT → Custom Lock Display → Tor

1. To whom should we attribute each attack?
2. How consistent are any two attacks with the same attribution?

Two Dimensions of Attribution



Horizontal: which attacks show similarities likely to result from the same perpetrator? → share forensics for attribution

Vertical: to which perpetrator should we attribute each attack?

Overview

- Key thesis
- **Getting Data**
- Formalizing the Model
- Applying the Model to the Data
- Next Steps

Active Case Solicitation

Example posting

As part of a research project under one of the usual funders of unclassified basic research in the US, we are compiling a census of actual ransomware attacks, with the objective of detecting possible clues to attribution. A unique feature of this census is using linguistic tools to examine the dialog structure of each attack—how the attack unfolded as a conversation between the attacker and the victim. We do not need to know the identity of the victim, but do have a list of questions that we would like to pursue in a phone conversation with individuals willing to share their experiences. These questions concern the participants in the unfolding attack (characteristics of the victim; type of system infected; point of entry; what is known about the attacker or attackers; payment method and destination; whether and how law enforcement was involved), as well as the time-sequenced series of utterances among the participants. The study will be completed by the end of 2017, and a summary report will be made available to those who have contributed their experience to the census. If you would like to participate, please contact us by private message on this website, or at radarproject2017@gmail.com . The prime contractor for this effort has asked that we use a project-specific alias, but Lawrence Abrams at Bleeping Computer has reviewed the details and approved this post, and we are happy to disclose the funding agency to individuals who contribute to our study.

Sites Posted

https://www.bleepingcomputer.com/forums/t/646823/ransomware-survey/#entry4240779

http://www.antionline.com/showthread.php?289129-Ransomware-Survey&highlight=ransomware

https://www.csiac.org/groups/cybersecurity/forum/ (submitted, but has not appeared)

Sites Evaluated

- Reddit, Topix: too diffuse, non-technical
- Symantec, McAfee, Alienvault: discussions are all product-focused

→ **No responses.**

Resources for Case Foraging

The Motherlode: http://goo.gl/b9R8DE

- "Ransomware Overview" spreadsheet led by Mosh (twitter @nyxbone, www.nyxbone.com, in Columbia)
- Extensive details on 405 varieties of RW, with links to further descriptions, screenshots, filename extensions, encryption algorithm used, link to decryptor if available, sandboxed version, IOCs, Snort rules, …
- Includes links to more detailed descriptions at BleepingComputer, PhishLabs, PhishMe, ProofPoint, MalwareBytes, PaloAltoNetworks, …

Campaign-level summaries (e.g., from RO spreadsheet), e.g.,

- http://www.securityweek.com/bart-ransomware-doesnt-require-cc-server-encrypt-files
- https://blog.malwarebytes.com/threat-analysis/2016/03/cerber-ransomware-new-but-mature/
- https://www.proofpoint.com/us/threat-insight/post/jaff-new-ransomware-from-actors-behind-distribution-of-dridex-locky-bart
- http://blog.trendmicro.com/trendlabs-security-intelligence/jigsaw-ransomware-plays-games-victims/

Individual attack reports on help forums (Malwarebytes, BleepingComputer, …)

Initial Set of Attacks

Attack	Appeared	Example Distinctives	Example Description
Bart	June 2016	Local encryption via zip files	http://www.securityweek.com/bart-ransomware-doesnt-require-cc-server-encrypt-files
GoldenEye initial	Jan 2017	Distribution via fake job application	http://www.zdnet.com/article/this-ransomware-targets-hr-departments-with-fake-job-applications/
GoldenEye derivative	June 2017	Distribution via SW update	https://labs.bitdefender.com/2017/06/massive-goldeneye-ransomware-campaign-slams-worldwide-users/
Jigsaw	April 2016	Incrementally deletes files if ransom not paid	https://www.bleepingcomputer.com/news/security/jigsaw-ransomware-decrypted-will-delete-your-files-until-you-pay-the-ransom/
Petya	April 2016	Encryption of master file table rather than files	https://blog.checkpoint.com/2016/04/11/decrypting-the-petya-ransomware/
Petya with Mischa	May 2016	Petya with fall-back conventional encryption	https://www.bleepingcomputer.com/news/security/petya-is-back-and-with-a-friend-named-mischa-ransomware/
WannaCry	May 2017	Breach via Eternal Blue NSA exploit; kill switch	https://www.bleepingcomputer.com/forums/t/646476/wannacry-wncry-wanacrypt0r-wana-decrypt0r-ransomware-help-support-topic/?hl=%20ransomware%20%20safari

Overview

- Key thesis
- Getting Data
- **Formalizing the Model**
- Applying the Model to the Data
- Next Steps

Backbone of an RW Attack

	Attacker / Computer	Third Party	Victim's Computer	Victim	Dooley Graph Analysis
1	→		→		(Breach System: Phish, Intercept, Penetrate)
2			↻		(Apply coercion: lock, encrypt, exfiltrate)
3	→	→	→	→	(Announce attack: files, notes, wallpaper, …)
4	←	Bitcoin ←	←	→	(Obtain payment: email, website, BC addr)
5	→	→	→		(Release coercion)

High-level stages derived by Dooley graph analysis (designed for analyzing dialog in natural languge)

Each stage offers multiple alternatives with different discourse structures

Need to distinguish at least the four domains shown (including multiple third parties) as discourse participants

Co-attribution is more likely if two attacks share TTPs for each stage.

H. V. D. Parunak. Visualizing Agent Conversations: Using Enhanced Dooley Graphs for Agent Design and Analysis. In *Proceedings of Second International Conference on Multi-Agent Systems (ICMAS'96)*, pages 275-282, 1996.

Three Ways to Breach

All *start* with attacker and *end* with victim's computer.

	Attacker / Computer	Third Party	Victim's Computer	Victim	Dooley Graph Analysis
	Website Intercept (Alma? Via RIG EK)				
1	→				(Intercept commonly used website)
2		Website	←		(Access website)
3			→		Respond(2) (expect Resolve to Victim)
	Phishing (e.g., BART, Cerber)				
1	→				(Task botnet)
2		Botnet	→		Respond(1)
3	←				Reply(2)
4	→		→		Respond(3)
	Direct Penetration (e.g., Apocalypse, Wannacry)				
1	→		→		

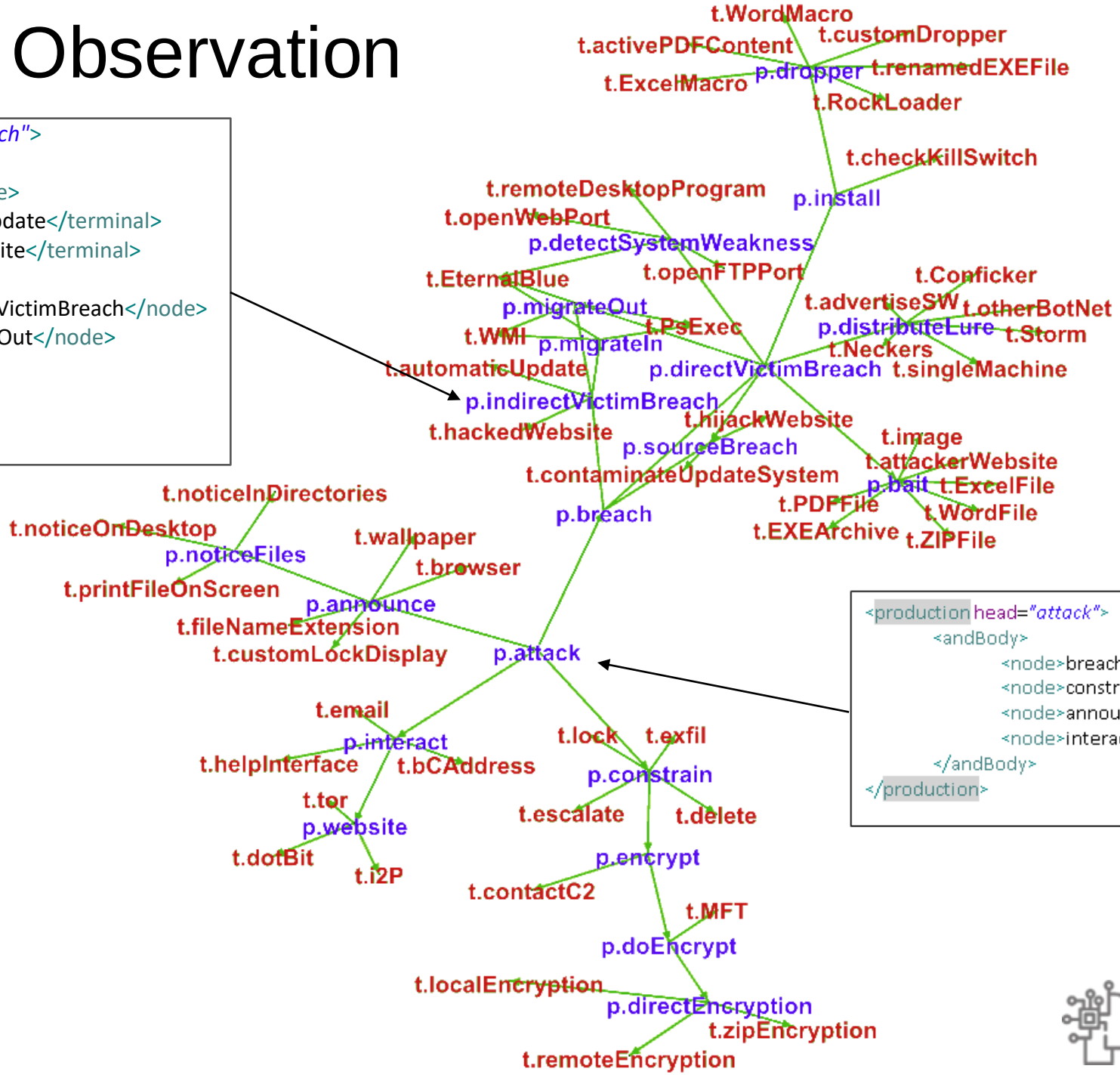
Three Ways to Interact

	Attacker / Computer	Third Party	Victim's Computer	Victim	Dooley Graph Analysis
	Leave Email Address (e.g., Dharma)				
1					(filename, .txt/.png file, wallpaper, …)
2					Resolve(1): Request instructions
3					Resolve(2): Send instructions
4		Bitcoin			Resolve(3): Get & deliver payment
	Website (e.g., BART)				
1					(website in wallpaper or file)
2					Resolve(1)
3					Resolve(2)
4		Bitcoin			Respond(3)
	Bitcoin Address (e.g., Jigsaw)				
1					(BC addr in file/wallpaper)
2		Bitcoin			

I'm guessing about the internal structure of email & website exchanges.

Simplifying Observation

```
<production head = "indirectVictimBreach">
    <orBody>
        <node>migrateIn</node>
        <terminal>automaticUpdate</terminal>
        <terminal>hackedWebsite</terminal>
        <andBody>
            <node>indirectVictimBreach</node>
            <node>migrateOut</node>
        </andBody>
    </orBody>
</production>
```




```
<production head="attack">
    <andBody>
        <node>breach</node>
        <node>constrain</node>
        <node>announce</node>
        <node>interact</node>
    </andBody>
</production>
```

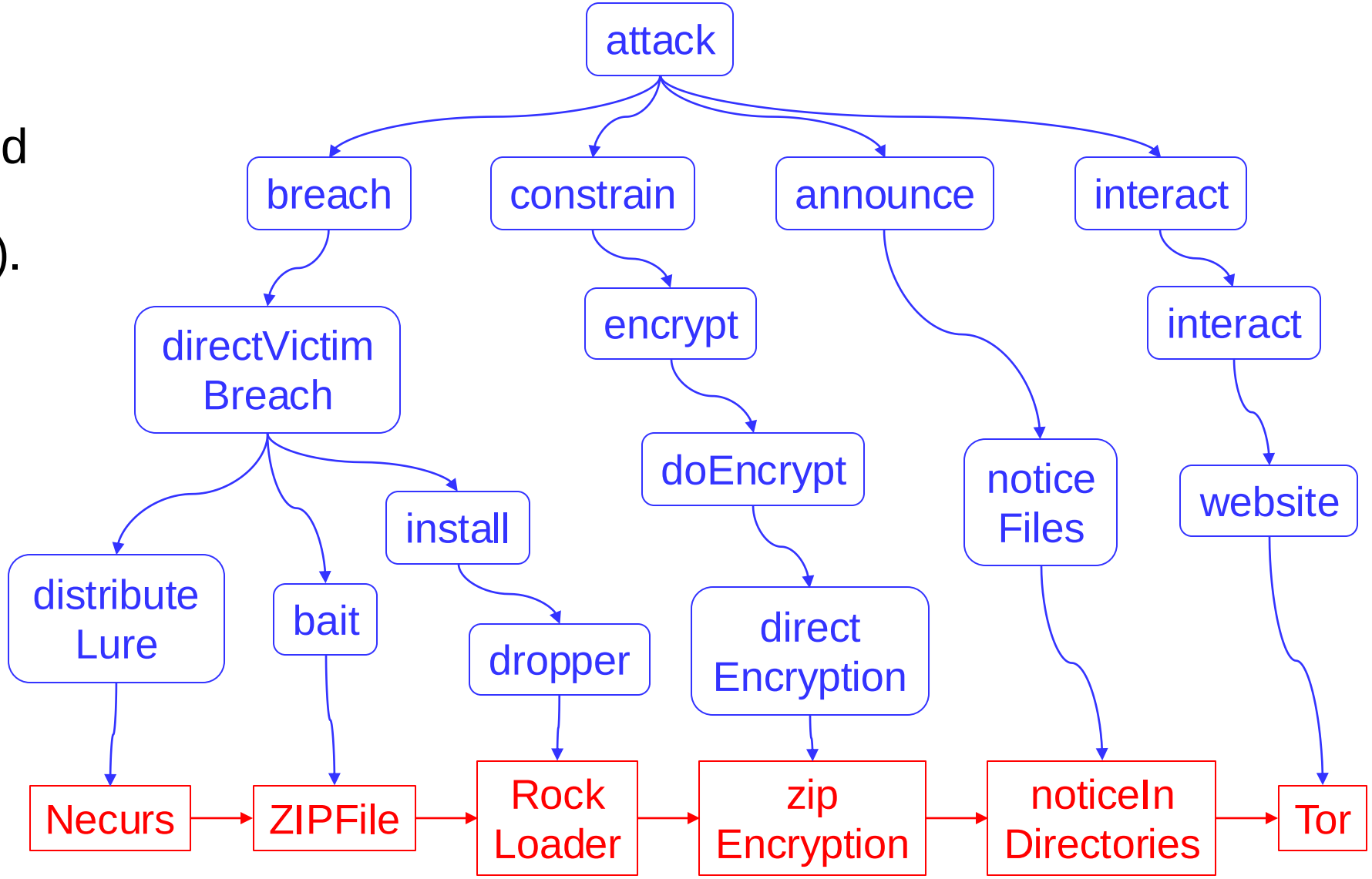
- Most of the variation is in the *sequence of actions*, not the *actors.*
- We can capture this efficiently in a context-free grammar.
- In graph, t.xxx is terminal, p.xxx is production.

Overview

- Key thesis
- Getting Data
- Formalizing the Model
- **Applying the Model to the Data**
- Next Steps

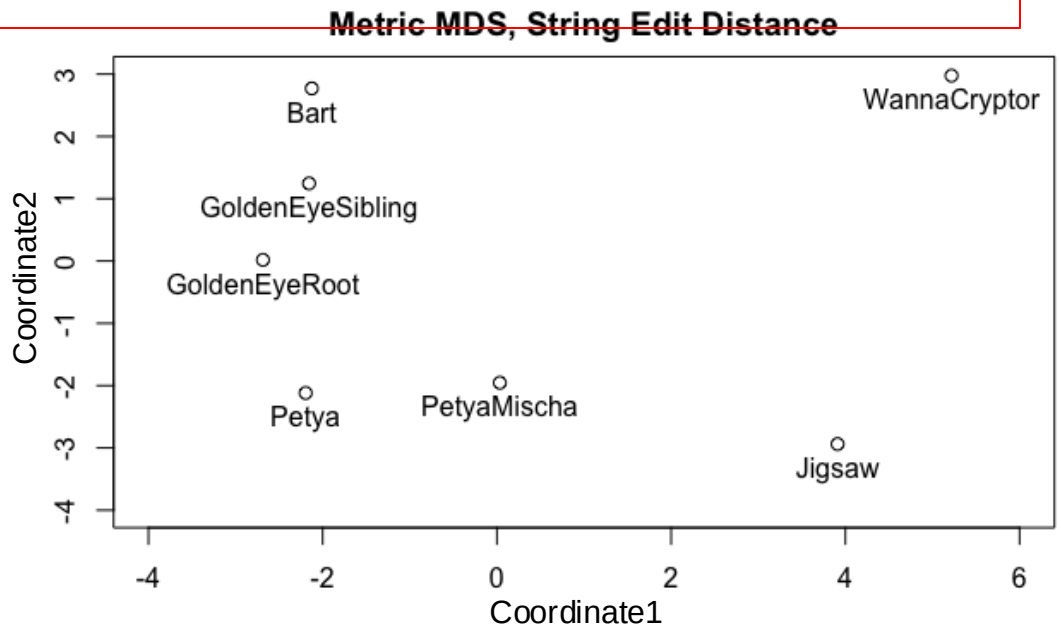
Applying the Model

Attack = Series of actions, each generated by a path through the grammar (our analysis). E.g., BART:



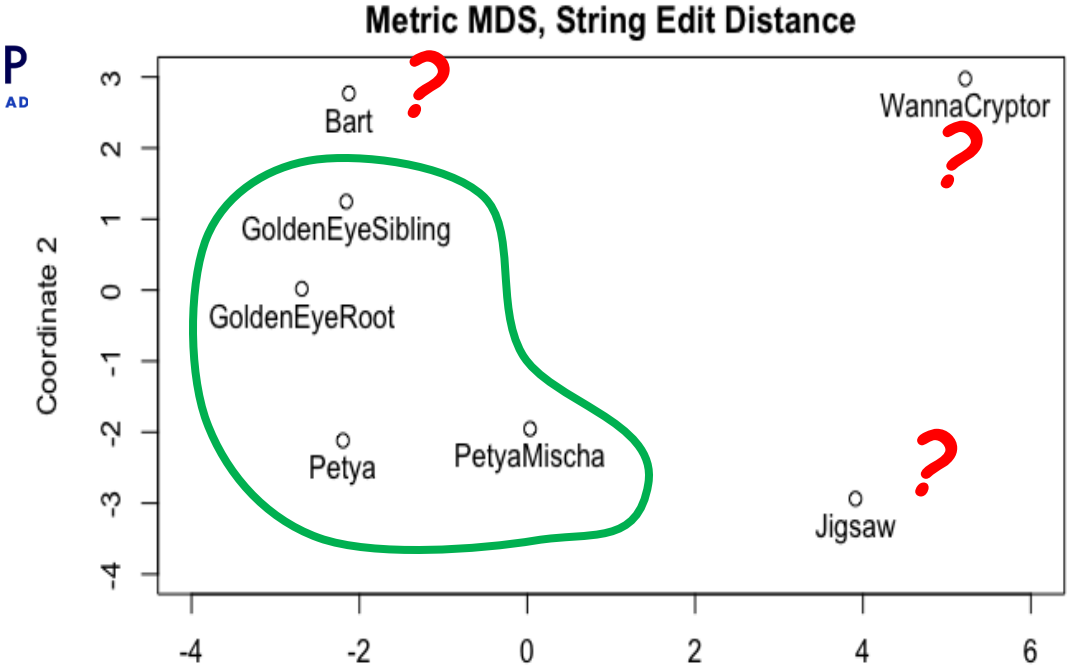
Similarity Measures between Attacks

Intuition: The more *similar* two attacks are, the more credible it is to *attribute* them to the same source.

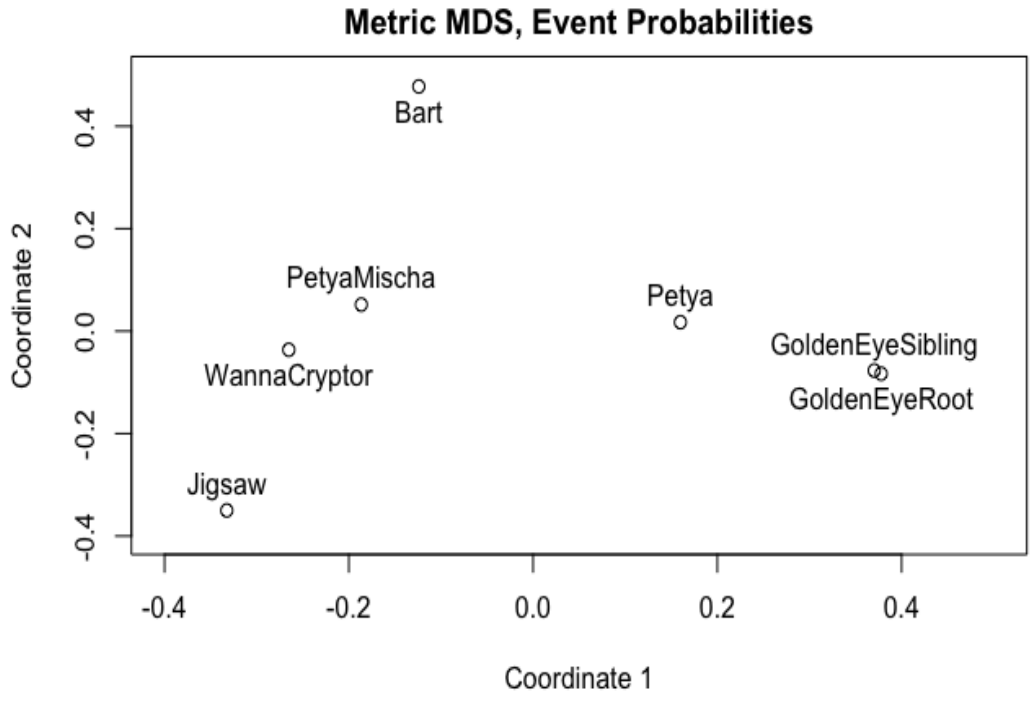


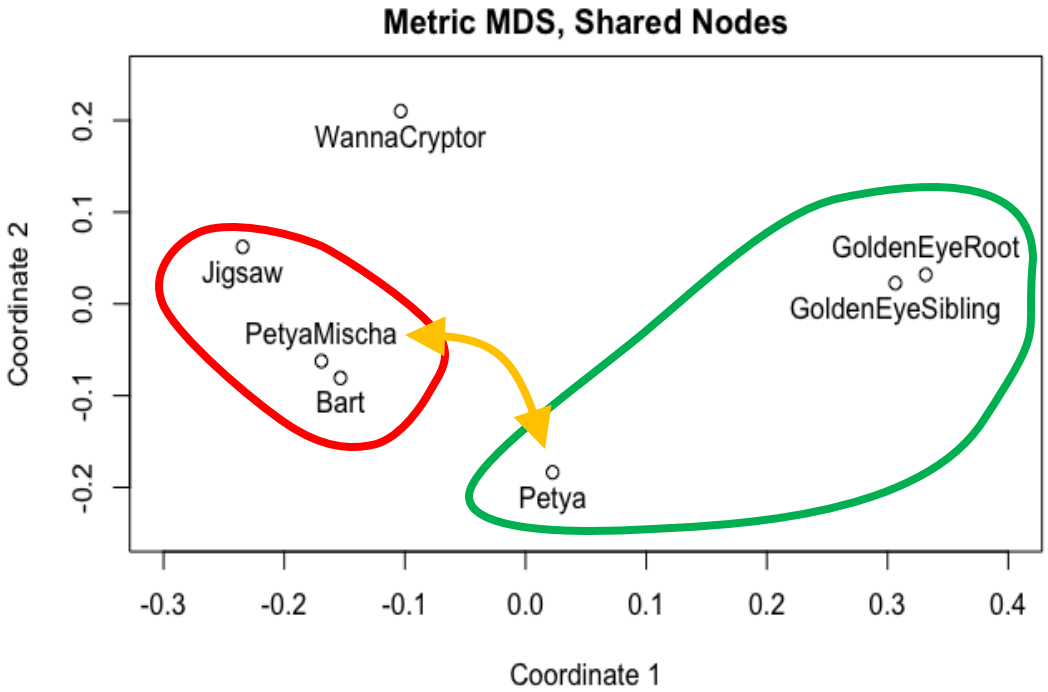
- String edit (Levenshtein) distance: ignores the path to a terminal (which we know from forensics)
- Grammar-based distance
  - Via **Lempel-Ziv compression**: widely used in comparing DNA sequences. Unlike our case,
    - Assumes repeated terminals
    - Grammar initially unknown
    - Unknown alignment
  - **Shared nodes**: $\frac{2*|sharedNodes|}{(|nodesInHistory1|+|nodesInHistory2|)}$
    - Assumes equal data and analysis on all branches
  - **Probabilistic** analysis: joint probability of the events being compared, *conditioned on any shared prefix*.

Measures for Co-attribution



← Recognizes common features in Petya and GoldenEye





- Better representation of Petya-GoldenEye lineage
- PetyaMischa's position reflects use of conventional encryption rather than master file table

- Excellent Petya-GoldenEye relation → Attribute to same source
- Highlights distinctives of Jigsaw (progressive deletion) and Bart (using Zip encryption)

Overview

- Key thesis
- Getting Data
- Formalizing the Model
- Applying the Model to the Data
- **Next Steps**

Next Steps

- Move from static *grammar* to executable *causal graph* representation (poster 34)
- Analyze more attacks
  - Analyzed 7
  - We have data on > 400, as of 2017
  - This would be a great project for a research assistant
- Use *horizontal* comparison of attacks to fuse evidence in support of *vertical* attribution.

Discussion and Questions

H. Van Dyke Parunak, Ph.D.
Parallax Advanced Research
734 395 3253
van.parunak@parallaxresearch.org
van.parunak@gmail.com

http://clipart-library.com/clipart/1422294.htm

Papers:
https://www.abcresearch.org/abc/papers