noblis

For the best of reasons

Securing our Underlying Resources in Cyber Environments (SoURCE CODE)

IARPA SoURCE CODE Lightning Talk

Nathan Clark
Principal Investigator, Cyber Research Center
5 October 2023

Noblis: A Non-Profit Science and Technology Company

As an innovator within the federal government, Noblis is committed to enriching lives and making our nation safer while investing in the missions of tomorrow.

- Civil
- Defense
- Homeland Security
- Intelligence and Law Enforcement

A Sample of Our Customers

- CMS
- FBI
- DHA
- NASA
- DHS
- USDOT
- DTRA
- USGC and IC
- FAA
- U.S. Navy

Noblis Science, Engineering and Technology Capabilities

Artificial Intelligence/ Advanced Analytics	Digital Transformation	Applied Sciences	Cyber Security and Operations	Autonomous Systems	Modeling and Simulation	Systems Engineering	Environmental Science
Artificial Intelligence System Test and Evaluation	Application Integration	Public Health and Bioinformatics Services	Cyber Defense Analytics	Orchestrated Autonomy Solutions	Immersive Technology and Extended Reality Solutions	Model Based System Engineering	Environmental Remediation
Algorithm Development	Multi-Cloud Architecture Services	Genomic and Health Sciences Research	Vulnerability Research	Human-Machine Trust Engineering	Aerospace System Design and Visualization	Digital Twin/Engineering Services	Sustainable and Resilient Infrastructure
Decision Analytics Services	Software Solutions	Chemical, Biological, Radiological, Nuclear and Explosives Solution Engineering	Enterprise Risk Services	Machine Self-Organization Research	Combat System Optimization	System Test, Design and Operations	Alternative Energy Research and Modeling
High-Performance Compute Services	Enterprise Architecture Design and Deployment	Bio-Security and Surveillance	Zero Trust Architecture Solutions	Autonomous Systems and Robotic Systems Test and Evaluation	Network and Telecom Services Modeling	System Integration Services	
Identity Intelligence System Development	Robotics Process Automation and Automation Services						
Multimedia Dataset Engineering	Digital Design and User Interface/User Experience Services						
Condition-Based and Predictive Maintenance							
Explainable Artificial Intelligence Research							

Noblis Mission Management Services

Economic Forecasting	Agile Program Management Office Transformation	Full Stack Acquisition Services	Innovation Management	Mission Operator Training

Physical and Virtual Innovation Spaces

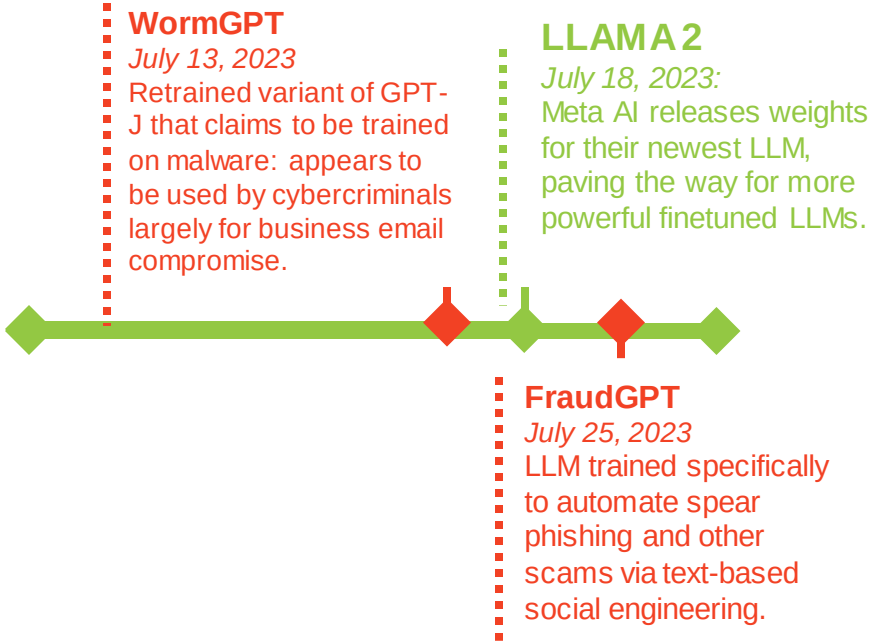
Machine Learning	Augmented Reality/Virtual Reality	Forensics and Biometrics	Solution Demo Center	BSL2 Life Sciences Facility	Autonomous Systems	Cyber and Network Test and Evaluation Range	Countering Weapons of Mass Destruction

noblis

IARPA Challenge

Provide novel techniques to assist forensic experts in making determinations of the most likely attackers, based on coding styles.

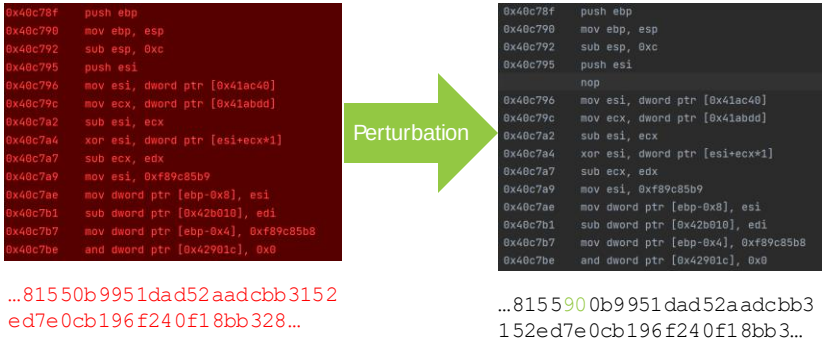
- How do we rigorously attribute malware to likely origins at scale?
  - Desire general means of determining likely origins of malware
  - AI-generated cyberattacks may require more general means of attribution



noblis

Key Considerations

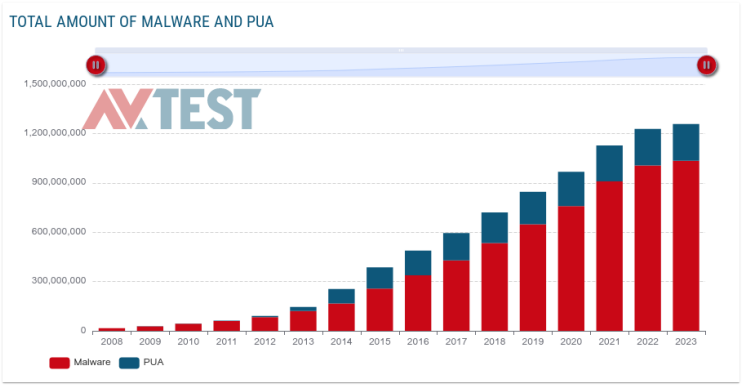
- General
  - Heuristics are often not general enough; e.g., signature-based methods are easily fooled by functionally-equivalent code
  - Previous Noblis research demonstrated the feasibility of automatically fooling dozens of malware detectors with a polymorphic engine



…81550b9951dad52aadcbb3152ed7e0cb196f240f18bb328…

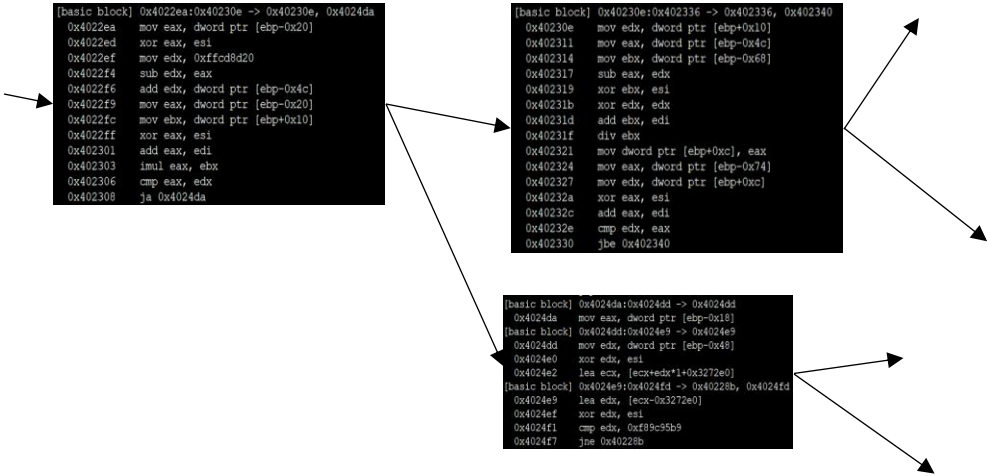
…81559000b9951dad52aadcbb3152ed7e0cb196f240f18bb3…

- Scalable
  - Known malware samples are on the rise, and AI-generated malware presents a considerable risk for accelerating the production of new cyberattacks
  - ML predictions can be learned automatically and cover far more general feature spaces

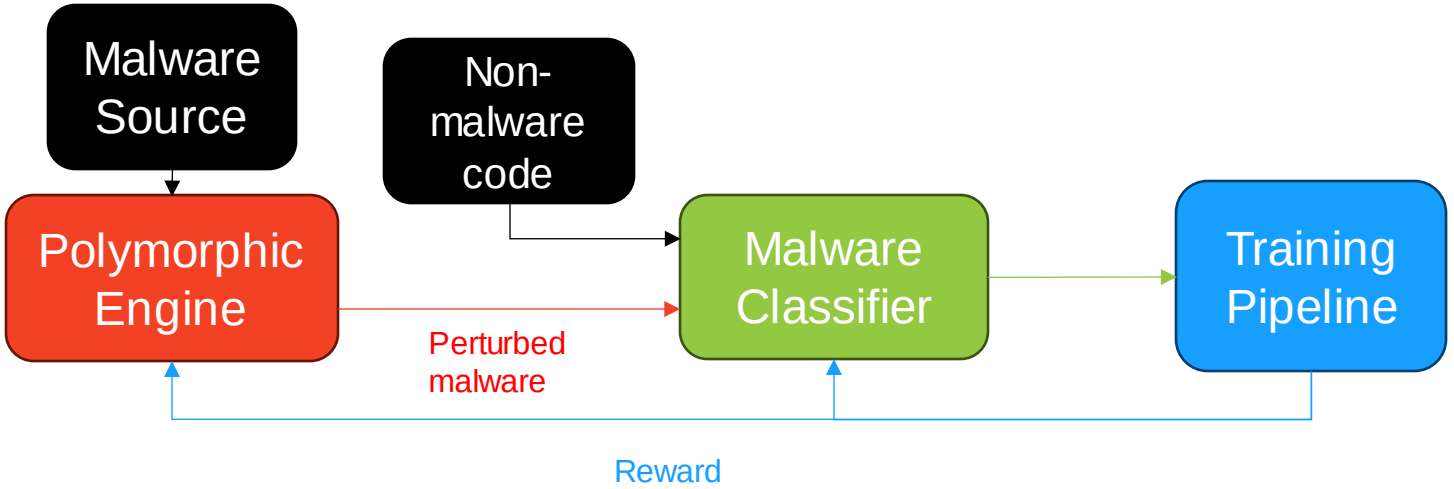


Noblis Approaches

- Graph convolutional network approach
  - Use control flow graphs on binaries
- Transformer approach
  - Especially helpful if source code (e.g. JavaScript) is available



Current Research



Given that existing ML approaches tend to overfit, Noblis research is based on adversarial learning between a model trained to generate perturbed malware and a malware classifier allowing for more rigorous detection

noblis

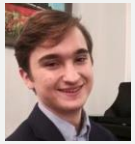
Looking Forward

- Create a capability to automatically cluster files by likely origins using ML
  - Leverage existing Noblis capabilities and infrastructure at the nexus of Cyber and ML
  - Siamese neural network to predict distance between malware samples in terms of likely origin feature space

noblis

Working With Us

Noblis partners with Government and Industry and Looks Forward to Hearing from You!



Nathan Clark
Principal Investigator, Noblis Cyber Research Center
Nathan.Clark@noblis.org, 703.554.2976

Patrick Hannon
ODNI Account Executive
Patrick.Hannon@noblis.org, 571.732.7684

Visit **noblis.org** to learn more

noblis.org/contracting

noblis