Hunting & Pivoting Using Research-Driven Threat Intelligence

Presented by Paul Makowski (@myhndl)
CTO & Co-Founder @ PolySwarm

POLYSWARM

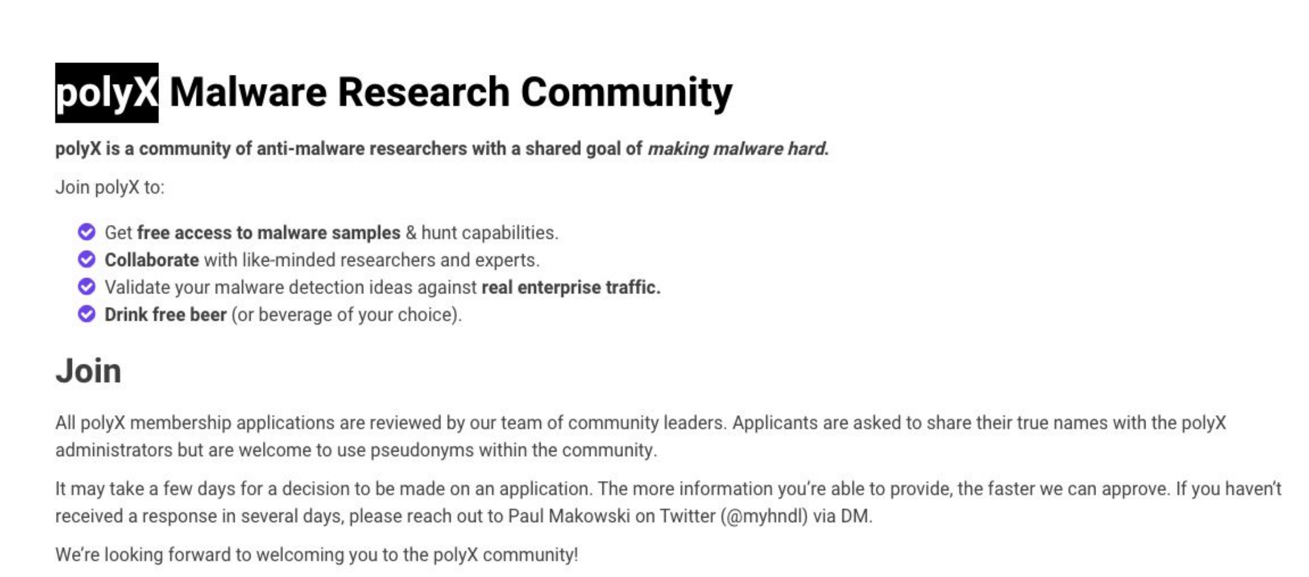
Agenda

- intro & polyX invite
- how PolySwarm works
  - researcher-driven engines, economic competition, PolyScore
  - feature overview: scans, searches, downloads, YARA
- hunting
  - Syrian COVID-19 malware
  - Iran’s AC19 app
  - coinminers using Zoom as a lure
  - Emotet
- metadata search deep dive
- wrap-up & join polyX!

polyX

Researchers making malware hard

- Free PolySwarm upgrades, malware & threat intel sharing
- join: https://go.polyswarm.io/polyx



polyX Malware Research Community

polyX is a community of anti-malware researchers with a shared goal of *making malware hard.*

Join polyX to:

- ✓ Get **free access to malware samples** & hunt capabilities.
- ✓ **Collaborate** with like-minded researchers and experts.
- ✓ Validate your malware detection ideas against **real enterprise traffic.**
- ✓ **Drink free beer** (or beverage of your choice).

Join

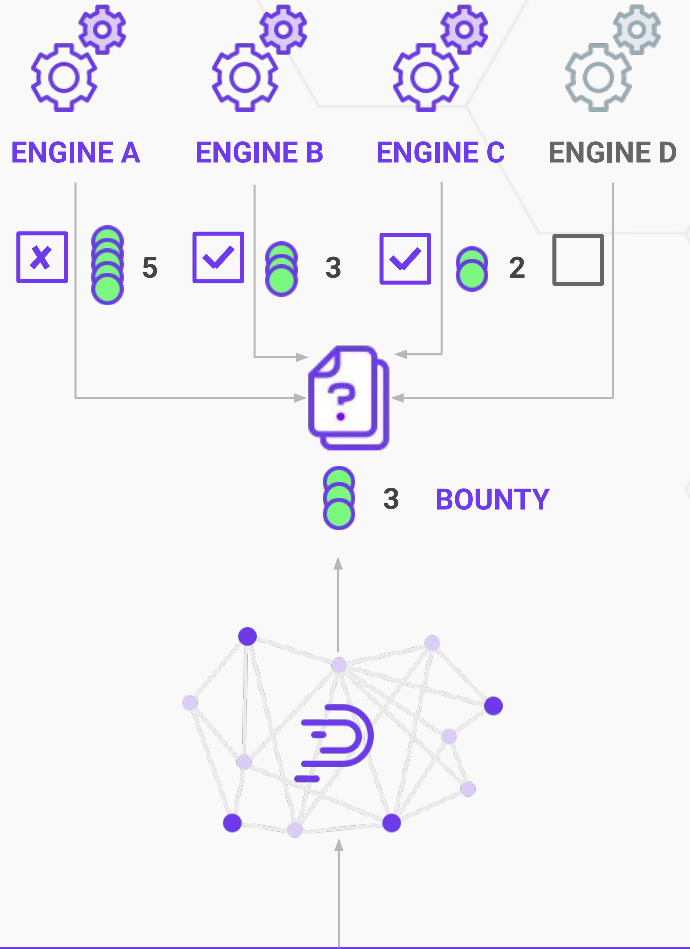
All polyX membership applications are reviewed by our team of community leaders. Applicants are asked to share their true names with the polyX administrators but are welcome to use pseudonyms within the community.

It may take a few days for a decision to be made on an application. The more information you're able to provide, the faster we can approve. If you haven't received a response in several days, please reach out to Paul Makowski on Twitter (@myhndl) via DM.

We're looking forward to welcoming you to the polyX community!

How PolySwarm Works

- Microengines scan all artifacts and provide assertions (malicious or benign) on some.
- They put their money on the line: Engines stake tokens along with their prediction, to keep them honest and signal confidence behind an 'opinion'.
- This process is automated and near real time, performed by software tuned by experts and infosec companies



Contextual Threat Scoring

PolyScore™

- **A single number with the probability a given file or URL is malicious**
- PolyScore’s algorithm aggregates engine’s opinions and **contextualizes their past performance resolving similar problems**
- Drives compensation model for research-driven engines
- PolyScore enables SOC and CTI automation

Let's Go Hunting!

POLYSWARM

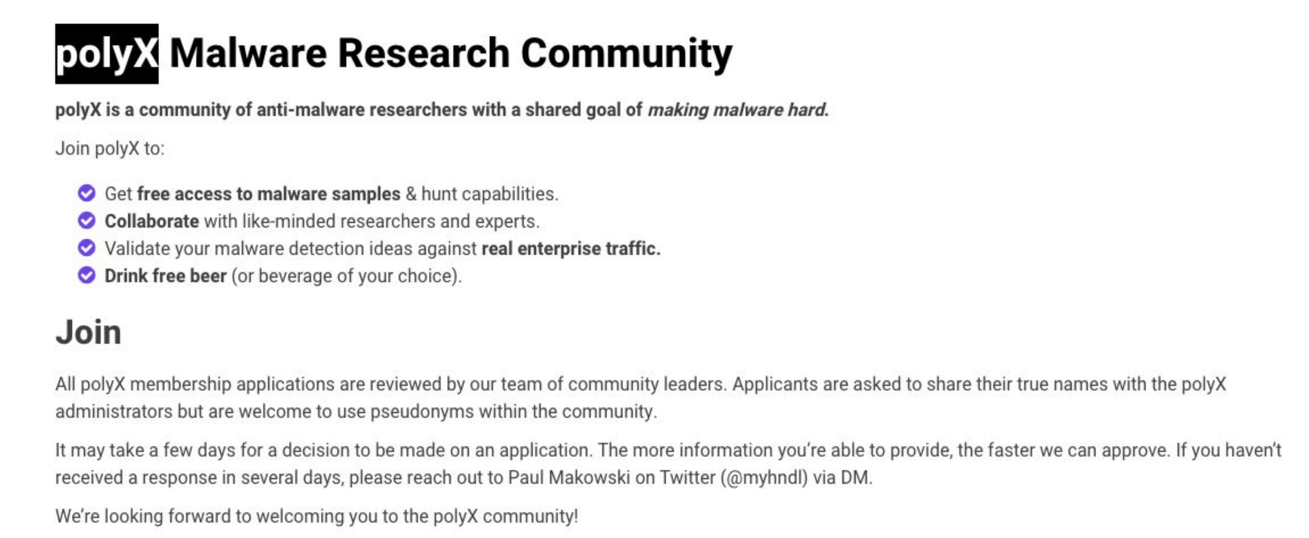
Agenda

- intro & polyX invite
- how PolySwarm works
  - researcher-driven engines, economic competition, PolyScore
  - feature overview: scans, searches, downloads, YARA
- hunting
  - Syrian COVID-19 malware
  - Iran’s AC19 app
  - coinminers using Zoom as a lure
  - Emotet (+ TrickBot & Ryuk)
- metadata search deep dive
- wrap-up & join polyX!

polyX

Researchers making malware hard

- Free PolySwarm upgrades, malware & threat intel sharing
- join: https://go.polyswarm.io/polyx



polyX Malware Research Community

polyX is a community of anti-malware researchers with a shared goal of *making malware hard.*

Join polyX to:

- ✓ Get **free access to malware samples** & hunt capabilities.
- ✓ **Collaborate** with like-minded researchers and experts.
- ✓ Validate your malware detection ideas against **real enterprise traffic.**
- ✓ **Drink free beer** (or beverage of your choice).

Join

All polyX membership applications are reviewed by our team of community leaders. Applicants are asked to share their true names with the polyX administrators but are welcome to use pseudonyms within the community.

It may take a few days for a decision to be made on an application. The more information you're able to provide, the faster we can approve. If you haven't received a response in several days, please reach out to Paul Makowski on Twitter (@myhndl) via DM.

We're looking forward to welcoming you to the polyX community!

Thank You!

Try out PolySwarm at: https://polyswarm.network

& learn more at: https://polyswarm.io

POLYSWARM