UNKNOWN CYBER

ABOUT

HEADQUARTERS
Lafayette, Louisiana

WEBSITE
UnknownCyber.com

COMMERCIAL USE

- End-point Detection Resolution
- Threat Hunting & Investigation
- Predictive Collective Defense

USER BENEFITS

- Identify & Harden against unknown malware before the rest of the world
- Triage new suspects
- Resolve alerts that remain unknown faster
- Hunt the next variant with automated YARA rules
- API based for automation
- Upskill and accelerate analysts by automating hours of expert malware analysis to minutes
- Available on a single machine as an incident response kit

COMPANY OVERVIEW

Unknown Cyber detects, hunts and attributes previously unknown malware with no reputation history in global threat repositories.

Attackers enjoy an asymmetric time and cost advantage by automatically generating thousands of new “unknown” malware variants daily. Unknown Cyber solves this problem with its patented technology researched through DARPA’s Cyber Genome Project. Our automation of deep reverse engineering provides clients a time and information advantage by accurately attributing the code lineage of millions of malware in minutes or less at scale.

Own the Unknown! Enable your defenders to detect and attribute unknown variants in minutes instead of days, weeks, or months. Our Basic subscription with API access is the equivalent of adding 10 experts.

With Unknown Cyber you can prevent the next attack before it occurs!

TECHNOLOGY HIGHLIGHTS

Speed Unpack and attribute an unknown binary and create custom Yara rules in ~4-6 minutes.

Scale Perform automated investigations across millions of suspect files.

Accuracy Resolve alerts triggered by your SIEM & SOAR faster.

Advantage Convict malware variants days to months before industry catches up.

Products + Packaging	Cloud	On-Premises	Incident Response Kit
EDR Integration	✓	✓	
Unpacking & De-obfuscation	✓	✓	✓
Reverse Engineering	✓	✓	✓
Attribution Automation	✓	✓	✓
YARA Creation Automation	✓	✓	✓
Suspect IOC Capture & Matched Variant IOC Delivery	✓	✓	✓
Malware Family Relationships	✓	✓	✓
Single Machine Deployable			✓

*Cyber Genome Technology identifies Future-Day ™ malware variants by defeating polymorphism and conducting automated reverse engineering to provide new variant conviction with code attribution confidence up to 100%.

CHALLENGE

Malware is easy to change to avoid detection. It is estimated that 70% of malware go undetected in the first hour with thousands remaining unknown for months after an attack.

SOLUTION

Detect malware by tracing its lineage in minutes.

Use unique and identifying shared code to create Yara rules for detecting the next unknown variant.

IMPACT

Gain a time, cost, and information advantage by automating days of expert work to minutes! One day of Unknown Cyber automation is the equivalent of a year of expert analyst work.