HEROIC
.com

Cybersecurity Powered by Artificial Intelligence and the Blockchain

HEROIC.com Team
February 2018

Abstract

HEROIC.com is powering the future of cybersecurity with artificial intelligence and the blockchain to protect against current and next-generation cyber threats.

As cyber threats are growing at an exponential rate, modern cybersecurity solutions are reactive, outdated, and ineffective. (1) The vast majority of threat data is controlled by large corporations and governments, making it difficult and costly to build next-generation solutions that improve protection. Recent advances in artificial intelligence based threat protection are promising, but the solutions are almost exclusively deployed to large corporate applications, which puts the technology out of reach of the people who are most vulnerable to attacks.

HEROIC.com is taking a new approach to AI-powered threat protection. Utilizing big data, artificial intelligence and the blockchain, combined with a decentralized peer-to-peer threat protection platform, HEROIC.com will change cybersecurity as we know it and make next-generation solutions freely available to everyone. HEROIC.com will empower and incentivize developers and companies to create the next generation of cybersecurity through the HEROIC.com Ecosystem, which includes an open threat intelligence exchange called HEROIC Arc Reactor™, a unified security management platform called HEROIC Guardian™, and a Research and Development environment. The motivation for collaboration within this Ecosystem will be incentivized through the blockchain and the use of HEROIC.com's cryptocurrency, the HRO (pronounced hero).

This paper presents multiple new and unique technologies specific to the HEROIC.com Ecosystem, including Threat Mining™, Cyberlytics™ and the Proof-of-Threat™ protocol. We anticipate thousands of potential applications for which the data provided can be used. An open, blockchain-powered cybersecurity ecosystem will unlock the massive opportunity for next-generation threat protection, eliminate the friction and costs from third-party intermediaries, and provide for a safer world.

We believe the combination of cyber threat data integrated with artificial intelligence and the blockchain is the future of AI-powered cybersecurity. The HEROIC.com Ecosystem and the HRO token will become a new standard used throughout the entire cybersecurity industry to globally ensure security, privacy and trust.

Notice: This document is for informational purposes only and does not constitute an offer or solicitation to sell shares or securities in HEROIC.com or any related or associated company or organization. Any such offer or solicitation will be made only by means of a confidential offering memorandum and in accordance with the terms of all applicable securities and other laws.

Notice: This document is for informational purposes only and does not constitute an offer or solicitation to sell shares or securities in HEROIC.com or any related or associated company or organization. Any such offer or solicitation will be made only by means of a confidential offering memorandum and in accordance with the terms of all applicable securities and other laws.

Table of Contents

1 The Problem with Current Cybersecurity Solutions

So much of our life hinges on trust in technology: Trust that when the light turns green, it's safe to go; that when we put our money into a bank or shop online, it's secure. Almost everything we use each day relies on technology, from alarm clocks and toasters to kids' toys and cars. It is estimated that by 2020 there will be more than 30 billion devices connected to the Internet. (2)

Along with the exponential increase in technology, the world is seeing a similar increase in malicious attacks. (3) As devices continue to become more intelligent and interconnected, significant privacy and security risks are being introduced. Not only are our devices vulnerable to attack; the most important details of our lives are stored on these devices and related cloud services. These details range from our medical records to our banking information to private communications with family and friends.

Private information in the wrong hands can have catastrophic consequences. IBM's CEO Ginny Rometty said, "We believe that data is the phenomenon of our time. It is the world's new natural resource. ...cyber-crime, by definition, is the greatest threat to every profession, every industry, every company in the world." (4)

The universal level of insecurity and the real costs associated with data breaches and cyber-crime are staggering: "72% of larger businesses reported a cyber incident in the past year and nearly half (47%) of all US firms experiencing two or more". (5) In 2016, over three billion personal records were stolen and leaked to the Dark Web and over 100 million Americans had their medical records stolen. (6) Almost everyone in the world who is connected to the Internet has been affected by one or more data breaches.

The continued increase in threats shows no sign that it will slow down any time soon. In a Forbes article, Steve Morgan from CSO Online stated, "From 2013 to 2015 cybercrime costs quadrupled, and it looks like there will be another quadrupling from 2015 to 2019. Juniper Research recently predicted that the rapid digitization of consumers' lives and enterprise records will increase the cost of data breaches to $2.1 trillion globally by 2019, increasing to almost four times the estimated cost of breaches in 2015" (7).

Current solutions are unable to keep up with the increasing number and intelligence of the threats attacking our systems. The signature-based threat detection systems commonly used today fail to detect new, previously unseen threats. Although effective if the threat vector is known and signatures are fully updated, these reactive solutions cannot protect us against the next generation of intelligent attacks. From self-driving cars to medical implants to general artificial intelligence (AI), the future of malware and intelligent systems will begin to attack the technology to which we entrust our lives and the lives of our loves ones. Over the last few years,

significant advances have been made with AI-powered threat protection, but that technology has yet to reach the masses. Next-generation solutions are almost exclusively focused on solving problems for the enterprise, with very little focus on individual users, families, or small to medium-sized businesses.

In addition to a focus on the enterprise, cyber threat data, which is the core component necessary to build intelligent algorithms, is primarily controlled and stored by governments and large corporations. Access to this data is paramount but prohibitively expensive, making it difficult for developers and small organizations to build next-generation, AI-powered solutions.

It is clear that incremental improvement is not sufficient to protect against the danger at our doorstep. Radical innovation is imperative … something HEROIC.

2 Ecosystem Overview

The HEROIC.com Ecosystem (the "Ecosystem") is an open, intelligent and incentivized cybersecurity ecosystem based on the blockchain, that protects against current and next-generation cyber threats. The core components of the Ecosystem are:

1) a decentralized cyber threat intelligence platform called ***HEROIC Arc Reactor™*** ("Arc Reactor");
2) a cloud-based unified threat management system called ***HEROIC Guardian™*** ("Guardian"), and;
3) a ***Research and Development Environment*** ("R & D Environment") for developers to develop and test their own algorithms on a secure, hosted platform. These three key components are integral and comprise the Ecosystem.

This is a unique approach to creating a long-term, sustainable and constantly evolving ecosystem for cyber threat protection. Once fully operational, the Ecosystem will provide the resources needed to protect intelligently against both current and next-generation threats.

2.1 Arc Reactor

HEROIC Arc Reactor™ is an open, decentralized cybersecurity threat intelligence exchange powered by the blockchain. Arc Reactor's purpose is to provide an open repository of cyber threat intelligence, simple programmatic access to the data, and an efficient marketplace for the data.

Data providers include but are not limited to individual threat miners, open-source threat intelligence providers, organizations of all sizes, and data partners. Collected data passes through an extraction process to pull relevant attributes that are then normalized and saved in a distributed database. The collected data along with its attributes are then ready to be used to train machine learning algorithms which will ultimately allow scoring and classification of samples.

Access to the collected samples and their attributes will be available programmatically via APIs and SDKs conforming to industry standard formats.

Arc Reactor will become more intelligent and robust as more users, organizations and data providers join the Ecosystem. We expect the data provided by Arc Reactor to power many cybersecurity-related products and eventually to become the world's largest repository of cyber threat intelligence.

A decentralized and open threat intelligence exchange will break down the barriers of entry when building AI-powered cybersecurity solutions, and will enable threat data to be distributed for universal benefit.

The marketplace for the data provided by Arc Reactor is exclusively powered by the HRO token and its related smart contracts.

2.2 Guardian

HEROIC Guardian™ is a unified, cloud-based cybersecurity platform. It provides a simple, online interface for individual users, families and businesses to manage all the pieces of the cybersecurity puzzle. Guardian utilizes the threat data from Arc Reactor and combines it with artificial intelligence to predict and prevent cyber-attacks.

Guardian will enable software developers and organizations to develop additional integrations and apps that connect with Guardian and its data layer. These integrations will enable developers to grow and monetize their creations, leading to a still more robust and holistic cybersecurity platform.

Guardian is provided as a freemium service with additional integrations and third-party services provided at an extra cost. Users can pay for premium services using HRO tokens or fiat currency. Guardian will also provide access to a secure wallet to manage HRO tokens.

2.3 Research and Development Environment

The R & D Environment will provide developers, organizations and companies alike with a central location to visually and programmatically interact with real-time and historical threat data provided by Arc Reactor.

Developers can research, develop and test their own algorithms in a secure, hosted environment. The environment will also provide access to community contributed algorithms and software to analyze and block threats, with the capability to turn overwhelming and disparate data into actionable insight and intelligence.

HEROIC.com is dedicated to providing the data, tools, and software necessary to build the next generation of AI-powered cybersecurity. We will help facilitate and incentivize the development of open-source software solutions as needed, with the first of them being open-source AI-powered threat protection.

Access to data and resources on the R & D Environment will be exclusively through the HRO token.

3 Ecosystem Participants

3.1 Individuals (Users and Threat Miners)

Individuals participating in the Ecosystem will be provided with multi-functional software that includes AI-powered threat protection, threat mining functionality, a secure wallet for HRO tokens and a connection to the Ecosystem.

Not only will users be able to protect their devices with the software, but they will also earn HRO tokens as their system finds, analyzes and shares anonymized threat data. As more users join the Ecosystem, larger amounts of data can be analyzed by the community's machine learning algorithms, which then makes everyone more secure.

The software will be available for most devices, including desktop computers, laptops, smart phones and IoT devices. Management of the software is through Guardian. Computing power, data storage and the data contributed to the Ecosystem is compensated with the HRO token and passes through an anonymity shield which strips it of any personally identifying information (PII).

Threat miners are those individuals who allow their devices to anonymously become part of the Ecosystem, forming a powerful collective of individual devices and computing power. The devices actively participating in threat mining receive compensation denominated in HROs for mined information and intelligence.

HEROIC.com will make it easy for users to participate without having to understand how the underlying technology works, and will provide online courses as a part of the Guardian platform.

3.2 Developers

Developers will have open access to the entirety of the Ecosystem. The core benefit for developers is the R & D Environment, which provides the opportunity to research, develop, test and distribute their own software and algorithms.

Developers will be compensated for their creations, which may include intelligent algorithms, software tools, and full software systems. Ecosystem compensation is made exclusively through the HRO token.

Additional benefits include:

- Access to one of the largest open-source cyber threat intelligence repositories
- A robust community of developers focused on cybersecurity and artificial intelligence
- The ability to visually and programmatically research, build and test proprietary algorithms using real-time and historical threat data

- Legitimate revenue streams to developers and security experts
- Compensation via the HRO token for data participation and most effective threat-blocking algorithms
- The ability to download and use the data for the developers' own cybersecurity research and products
- Compensation for the building of decentralized applications (Dapps) that interact with the ecosystem.

We anticipate that the Ecosystem will inspire talented people everywhere to write cybersecurity algorithms and build solutions for the greater good.

3.3 Organizations

Like developers, organizations will also have open access to the entirety of the Ecosystem for use in protecting their own data, receiving compensation for contributed data and integrating it with third-party branded products and services.

Organizations are an important part of the Ecosystem as they will help contribute vast amounts of data that help protect the entire Ecosystem and will provide for an efficient marketplace of threat data. Organizations may include businesses, schools, non-profits, mining-pools, governments and others.

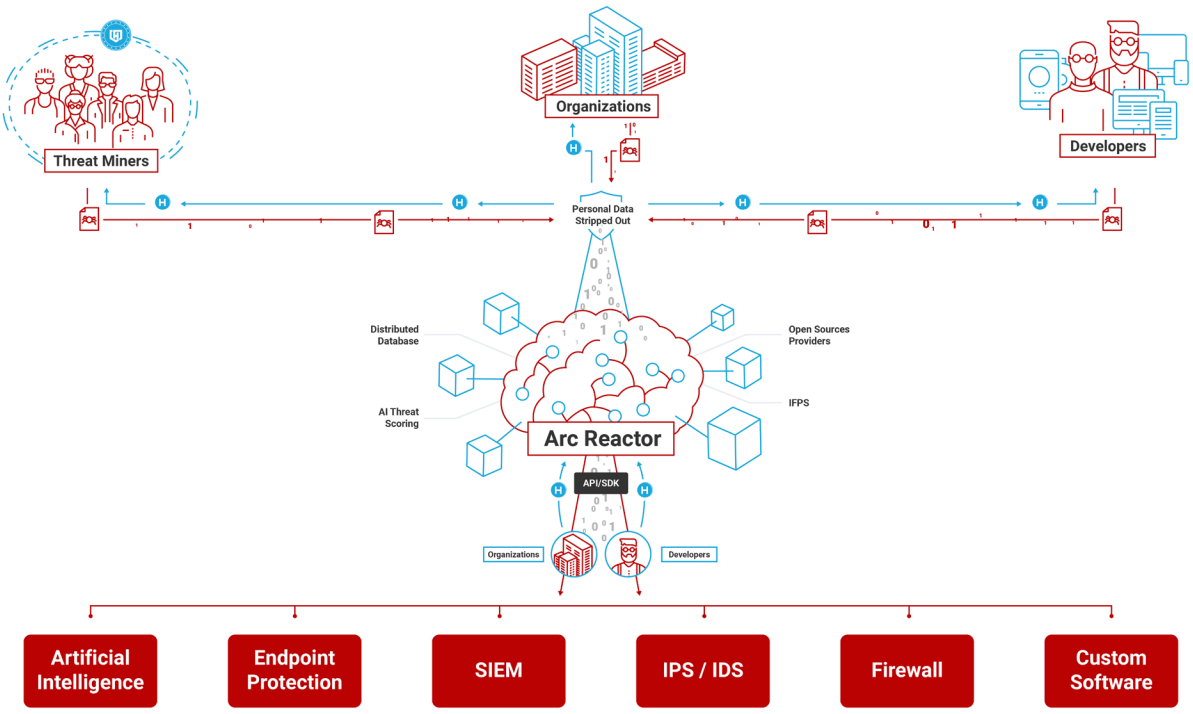
Using industry standard distribution methods, organizations will be able to consume the data for use with internal cybersecurity systems and to build their own software.

Benefits for organizations include:

- Access to one of the largest open-source cyber threat intelligence repositories
- Compensation for data participation and contributions to threat-blocking algorithms
- The ability to download threat data to enhance their own cybersecurity products
- Compensation for the building of decentralized applications (Dapps) that interact with the ecosystem.

4 Technology Overview

As described above, the HEROIC.com Ecosystem consists of three core projects that combine to make an effective security solution of benefit to all types of users, including individual users, developers and organizations. It has been designed to provide multiple levels of access, value and support in order to stimulate accelerated research, development and integration of advanced cybersecurity technologies, in addition to ensuring universal access to these technologies. The larger the Ecosystem grows, the stronger it will be.



4.1 Arc Reactor

Arc Reactor is an open and decentralized cybersecurity threat intelligence platform that provides three main functions. These are the collection, transformation and distribution of threat data, for use with artificial intelligence and cybersecurity systems. We consider each of the three functions below.

Collect

Threat data is collected from many sources, including threat miners, open source threat feeds, commercial threat intelligence providers, community-provided threat intelligence, and threat sharing from organizations. Each source participating in the Ecosystem is an autonomous agent, capable of performing these actions with limited human interaction.

Ecosystem participants will be provided with software agents and programmatic access to contribute a constant stream of threat data. Collected data passes through an anonymity shield to make sure that no personally identifying information is shared.

Transform

Collected threat data goes through a cleaning process which includes verification, normalization, de-duplication and enrichment. This cleaned data is then stored in a distributed storage network using IPFS, and metadata is stored in a distributed database.

Once stored, threat data will go through additional processes that associate, classify and score the data using artificial intelligence. This additional metadata associated with the sample is then merged with the metadata in the distributed database.

Distribute

Multiple threat data feeds will be provided to Ecosystem participants, including: File Details, Domain, URL & IP Data, Dark Web Data, IOC, and Community Data. Access to data feeds will be provided programmatically using industry standards via APIs and SDKs. These standards may include YARA, STIX, TAXII, CybOX and others.

Arc Reactor provides the big data and incentivization necessary to feed artificial intelligence that can ultimately be used to protect against threats. We expect that threat data will be used for many different applications, including AI-powered Endpoint Protection, Intrusion Detection/ Intrusion Prevention systems, Security Information and Event Management (SIEM), Botnet Detection, and Phishing Detection and Prevention.

4.2 Guardian

Multiple layers of security are needed to protect a user's technology. These layers include antivirus software, data breach monitoring, protection from identity theft, credential management, backups, DNS and many more systems. At HEROIC.com, we often call these layers the cybersecurity puzzle.

Guardian is a unified, cloud-based cybersecurity platform that provides a simple interface for individual users, families, and organizations to manage all the pieces of the cybersecurity puzzle.

Guardian will initially provide core layers of the cybersecurity puzzle while enabling developers and organizations to contribute, and be compensated for, integrations with the Guardian App Store. Guardian Apps will use developer APIs to interact with the Ecosystem data. These combined pieces will unify and simplify cybersecurity management.

Guardian combines artificial intelligence with the data from its interconnected applications and Arc Reactor to predict and prevent cyber-attacks. Guardian users will not only benefit from the overall intelligence provided from the Ecosystem but will also have their own personal AI dedicated to protecting their devices and cloud services. As more data is analyzed, the system will continue to get smarter and better protect against attacks.

The Guardian software stack consists of the following technologies:

- Cloud-based, unified cybersecurity management
- Software agents and data sensors
- Endpoint management
- Developer APIs
- App Store for third-party integrations
- User-specific AI engines
- Blockchain transaction management

4.3 Research and Development Environment

The R & D Environment provides simple access to Arc Reactor's threat data combined with robust research and software development capabilities.

Developers can learn about artificial intelligence and cybersecurity from our tutorials and lectures. Using that information, they can build and test their own creations against real-time and historical data in an Interactive Developer Environment (IDE). Developers will also be given incentives to build the best threat protection algorithms and to sell their technology in the marketplace in exchange for HROs.

The R & D platform will empower a community of developers and researchers with the knowledge and resources needed to build the next generation of threat protection.

The R & D Environment consists of the following technologies:

- Access to historical threat data
- Developer APIs
- Software testing sandbox
- Software tools
- AI and cybersecurity intelligence community
- HRO-powered marketplace
- Blockchain transaction management

4.4 Other Technology

4.4.1 Agent Software

The agent software can be installed on individual devices and provides a variety of functions including threat mining, ecosystem connections, endpoint protection, a secure HRO wallet, and simple system management.

The agent software will be available for multiple devices including desktops, laptops, mobile phones, and IoT devices. Agent software is expected to be developed for all popular operating systems.

Each individual agent actively monitors file actions and changes, ecosystem traffic, user behavior, and file attributes. Agents can independently identify anomalies and threats, validating them and taking appropriate action. This monitoring ensures the protection of the user as well as their data.

Communication within the Ecosystem is performed between the agents, Arc Reactor and the blockchain in order to characterize validated threats, grow the intelligence of the system, and arrange compensation for threats mined. Such communication also aids threat identification and validation, and ensures real-time inoculation from active attacks.

Verified threat data is anonymized and sent out to the ecosystem to help other systems prevent future threats and for developers to build their threat protection algorithms.

Once fully developed, the agent software may act as a device's primary endpoint protection, to identify and block threats in addition to providing processing power and storage to the Ecosystem for remote threat monitoring and identification.

4.4.2 Artificial Intelligence (Cyberlytics®)

HEROIC.com uses artificial intelligence as a general term to describe the many intelligent systems and processes that will be used within the Ecosystem.

Artificial Intelligence within cybersecurity encompasses many different fields of study including math, machine learning, neural networks, pattern recognition, anomaly detection and more.

Cyberlytics® is HEROIC.com's intelligent AI-based engine, used to predict and prevent cyber-attacks before they happen. The Cyberlytics engine analyzes tremendous amounts of complex threat data from Arc Reactor to create powerful insights that are used to automatically protect your technology, your data, and ultimately you.

4.4.3 Blockchain Software

HEROIC.com uses Ethereum smart contracts for transactions which facilitates direct payments between users, organizations, and software developers. By using a secure blockchain based ledger, HEROIC.com provides the ability to acquire, maintain and transfer HROs. We will continually incentivize and compensate users contributing to the Ecosystem, including making and receiving payments for distribution and usage of threat data.

Our consensus algorithm is proof-of-work based on Ethereum's proof-of-work protocol, which will eventually become HEROIC.com's novel Proof-of-Threat™ protocol.

4.4.4 Proof-of-Threat™

HEROIC.com's novel Proof-of-Threat™ protocol will eventually be used as the main method for quantifying the work completed by each node, and will provide a score to

each individual threat sample. Instead of wasting precious energy and resources to compute hashes, the Proof of Threat protocol will allow miners to contribute their computing resources to the analysis and scoring of potential threats, and to be proportionally compensated for that work.

Threat scoring provides a numerical value to each individual threat. The score indicates the probability of the sample being a threat. The higher the score, the more likely it is to be a threat.

Scoring of samples is beneficial as it provides systems with more control over whether or not to block the threat, instead of providing a simple binary value of whether something is or is not a threat.

A threat score is based on a number of factors and uses a weighted arithmetic mean to produce a score from zero to 100. HEROIC.com takes a machine-learning approach, initially scoring each sample on a node and then using Arc Reactor data to validate the initial score and learn from the data.

The Proof-of-Threat score will be calculated using some or all of the following systems.

- Pre-execution
  - HEROIC AI-powered Cyberlytics engine
  - Artifact hash comparison with known threats in Arc Reactor
- Post-execution
  - Heuristic artifact analysis that observes behavior or characteristics of a file or process which may indicate that it is suspicious.
  - Sandbox Analysis

The Proof-of-Threat™ protocol and threat scoring engine will be open-source and available to everyone. A more comprehensive whitepaper on the initial implementation of Proof-of-Threat™ will be released at a future time.

4.4.5 Data Pricing (Dynamic Pricing algorithm)

The pricing of the threat data is one of the most important aspects of the Ecosystem, as the system must motivate users to contribute data with its pricing structure while not turning away consumers of the data because costs are too high.

Instead of providing a bid–ask pricing system which adds unnecessary friction and complexity for users, we are building an automated, real-time pricing algorithm that motivates data providers by maximizing profitability, and motivates consumers of the threat data by providing hyper-competitive pricing. This system is similar to what Uber uses to provide pricing to its riders and drivers, as there is no need for user choice or explicit transparency in how the prices are determined.

The algorithm provides dynamic pricing based on supply of and demand for the data provided. It takes into account aspects such as the age and size of the data, its type and

its potential importance, the total size of the order, threat score, and other market conditions.

As we receive feedback from Ecosystem users and our understanding of the value of the data increases, we will continually update the algorithm and integrate machine learning to provide an ever more efficient marketplace.

The following is an example of the current mathematical notion that will be implemented.

$$F = M\left(\frac{X}{M + .BN + .CP}\right) + .BN\left(\frac{X}{M + .BN + .CP}\right) + .CP\left(\frac{X}{M + .BN + .CP}\right)$$

F = total monthly earnings for each threat miner
M = Data Type 1 (valued at A%) (as determined by other factors)
N = Data Type 2 (valued at B%) (as determined by other factors)
P = Data Type 3 (valued at C%) (as determined by other factors)
X = income earned from data consumers that month

5 Token Details

5.1 HRO Token

As part of the development of the HEROIC.com Ecosystem we are introducing the HRO token (pronounced hero), which will be used as a form of authorization, incentivization and settlement between participants on the Ecosystem, and for other related services.

A fixed supply of HROs will be created as a part of the token sale, with appropriate smart contracts and a blockchain-based ledger which will follow the ERC20 standard. The ledger will provide a secure method for HRO holders to hold and transfer HROs to other users.

While HEROIC.com intends to develop the initial software and smart contracts that power the Ecosystem, we expect the HRO to be a new standard that is used throughout the entire cybersecurity ecosystem and other industries.

5.2 Token Incentives & Benefits

The Ecosystem has been designed to provide multiple levels of access, value and support in order to stimulate accelerated research, development and integration of advanced cybersecurity technologies, and to ensure the availability of these technologies to everyone. Incentives are managed through the use of the HRO tokens with the Ecosystem being multi-transactional, allowing both purchases and payments between any combination of HEROIC.com participants, including end-users, developers, and organizations.

5.3 Token Market

HEROIC.com is building a robust market for threat data, powered by the HRO token. HROs may be purchased using Bitcoin (BTC), Ethereum (ETH), other popular cryptocurrencies, or fiat currency.

Users who own HROs may use their tokens to purchase existing and future services directly from HEROIC.com and other partners of the Ecosystem.

The token will be available in select cryptocurrency marketplaces. Ecosystem participants will each be provided with a secure wallet with which they can manage their HRO tokens.

5.4 User Growth Fund

A user growth fund will be implemented to incentivize users to participate in the various aspects of the Ecosystem. HEROIC.com will also incentivize and help facilitate the development of additional cybersecurity-related services that can be exchanged for HRO tokens.

6 Privacy & Security

With a project of the magnitude and importance of HEROIC.com's Ecosystem, a statement on the importance and application of privacy and security is required.

Privacy is of paramount importance to us. We will strive to maintain compliance with related regulations, including Data Loss Prevention (DLP), NIST guidelines, GRDP requirements, and other cybersecurity best practices. As such, data protection tools, process, and systems are paramount in ensuring the privacy of HEROIC.com's clients, and any stored data is maintained.

HEROIC.com strives to employ the latest cybersecurity technologies and standards, and will continue to evolve and be transparent about the technology it uses. HEROIC.com's policies are designed to ensure that stored data is not made available to unauthorized persons or organizations.

As a part of our cybersecurity plan we will maintain a bug bounty program for all aspects of our architecture, with bounties denominated in HRO tokens. It is important to note that our goal is eventually to host all aspects of the Ecosystem on zero-knowledge architecture.

In order to enforce ethical user standards, any participants or users who purposely cause damage to the Ecosystem, platforms, or applications, or use the data for unethical purposes, may be permanently denied access and may lose access to their HRO tokens.

7 Other HEROIC.com Technologies

HEROIC.com is a spin-off from a two-time Inc. 500 company specializing in enterprise cybersecurity and software development, and was founded with a mission to intelligently protect the world's information. With that mission, HEROIC.com has been actively involved in the development of a number of cybersecurity products. The following products are currently available and are being used by large organizations.

7.1 HEROIC DarkHive™

HEROIC DarkHive is one of the world's largest collections of leaked and compromised user credentials. HEROIC.com uses intelligent technology and cybersecurity analysts to scour the deep and dark web for hacks, leaks, and any other source of compromised data.

The DarkHive includes both detailed hack data as well as summary data, for use in enterprises around the world. The DarkHive is the large data repository that powers EPIC (see below).

7.2 HEROIC EPIC™

HEROIC EPIC helps to discover, remediate and prevent the use of stolen log-in credentials found in third-party data breaches and leaks.

In 2016 over 3.3 billion records, including email addresses, usernames and passwords from 1,700+ data breaches, were leaked onto the dark web. Once made public, hackers and other parties can obtain and use those records to brute force their way into organizations' systems and ecosystems, to carry out targeted attacks. EPIC discovers vulnerabilities and prevents attacks by obtaining the same leaked databases from the dark web and notifying organizations if their employee or customer data has been compromised. This gives security professionals an opportunity to fix stolen log-ins before they are used against their owners.

8 Future Work

The HEROIC.com team believes that to achieve our mission of providing next-generation cybersecurity to everyone, the current pace of development is insufficient to eclipse the rate of cyber threats, and therefore requires significant expansion and accelerated development.

As stated in the Abstract, we expect that there will be literally thousands of potential applications for which the data provided by the HEROIC.com Ecosystem can be used. We do not intend to build the vast majority of these applications, but to facilitate and motivate others on the Ecosystem to build these systems.

Funds raised from the token sale will be applied to the projects listed in this document, with the initial priority being to complete the HEROIC.com Ecosystem in order to provide users with a decentralized platform to manage all aspects of their cybersecurity needs.

This paper sets out a clear and cohesive path toward the construction of the Ecosystem. However, we also consider it to be a starting point for future research on AI-powered cybersecurity software.

Active research is continuous, and new versions of this paper will appear at HEROIC.com. For comments and suggestions, please contact us at contact@HEROIC.com.

8.1 On-going work

The following topics represent relevant ongoing work expected to provide significant benefit to the HEROIC.com Ecosystem

- **A fully implementable Proof-of-Threat protocol specification**
- **Research into emerging decentralized storage solutions**
- **Detailed performance estimates and benchmarks for the HEROIC.com Ecosystem and its components**
- **Machine learning algorithms for a more efficient marketplace for threat data**
- **Game theoretical analysis of HEROIC.com's incentives.**
- **Millisecond transactions via off-chain ecosystems similar to the Bitcoin-related** https://lightning.ecosystem/ **or Ethereum Raiden** https://raiden.ecosystem/
- **Integration with other blockchains**
- **Penalties for participants or users who purposely cause damage to the Ecosystem or any application, or who use the data for unethical purposes**
- **Zero-knowledge architecture**

9 Acknowledgements

This work is the cumulative effort of multiple individuals within the HEROIC.com team, and would not have been possible without the help, comments, and review of the collaborators and advisors of HEROIC.com. Chad Bennett is the original architect of the HEROIC.com Ecosystem. He and David McDonald wrote this whitepaper in collaboration with the rest of the team, who provided useful contributions, comments, review and conversations. Tammy Bennett helped improve the structure and wording of the paper while Wyatt Semanek created the illustrations and finalized the paper. Multiple crypto-related whitepapers were consulted in the preparation of this work and are referenced in the citations (8), (9), (10) and (11). We also thank all of our collaborators and advisors for useful conversations and support.

10 Appendix

Cybersecurity – A Short History

Glossary

AI-Powered: Software that uses artificial intelligence or machine learning algorithms, instead of a human, to make the software more intelligent.

Algorithm: a set of rules for solving a problem in a finite number of steps, as for finding the greatest common divisor.

Artificial Intelligence: The theory and development of computer systems able to perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages.

Big Data: Extremely large data sets that may be analyzed computationally to reveal patterns, trends, and associations, especially relating to human behavior and interactions.

Blockchain: See https://HEROIC.com/blockchain-overview

Cryptocurrency: A digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank or authority.

Cybersecurity: The body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

Data Mining: The process of discovering interesting and useful patterns and relationships in large amounts of data.

Decentralize: To disperse (something) from an area of concentration; to create something without limiting its control or use to a small group.

Democratized: To make accessible and open to everyone. Power is vested in the people and exercised directly by them.

Fiat Currency: Currency that a government has declared to be legal tender, but which is not backed by a physical commodity. The value of fiat money is derived from the relationship between supply and demand rather than the value of the material of which the money is made. Examples of fiat currency include the U.S. dollar, euro, British pound, etc.

HEROIC Arc Reactor: HEROIC.com's unified threat management platform, designed to bring together the intelligence and data of the cybersecurity world.

HEROIC.com Ecosystem: The newest system or network of interconnecting and interacting parts, to help protect the world from cyber threats as fast as they are created, or faster. The system will employ three new platforms together to create fast, up-to-date, and proactive cybersecurity solutions for everyone.

HEROIC Guardian: A unified, cloud-based platform created by HEROIC.com to help protect users from cyber threats, using artificial intelligence.

Machine Learning: The ability of computers to learn without being programmed. Makes predictions on data.

Threat Miner: Users of HEROIC's threat mining software who search for, validate and distribute threats to the network.

Threat Protection: a service or system that helps protect you or your company from problems or malicious attacks.

Zero-Knowledge Architecture: Software architecture where the storage of data on systems is encrypted with public and private keys in such a way that the storage provider does not have access to decrypt or view the data.

11 Citations

1. BITSIGHT. Thousands of Organizations Run The Majority of Their Computers on Outdated Operating Systems, Nearly Tripling Chances of a Data Breach. Press Release. [Online] https://www.bitsighttech.com/press-releases/thousands-organizations-run-majority-of-computers-on-outdated-operating-systems.

2. Claveria, K. 13 stunning stats on the Internet of Things. [Online] October 24, 2017. https://www.visioncritical.com/internet-of-things-stats/.

3. Internet Security Threat Report. [Online] Symantec, April 2016. https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf. Volume 21.

4. Rometty, G. IBM Security Summit. . [Online] May 4, 2015. https://www.ibm.com/ibm/ginni/05_14_2015.html.

5. Hiscox. The Hiscox Cyber Readiness Report 2017. [Online] 2017. http://www.hiscox.com/cyber-readiness-report.pdf.

6. Graham, Luke. Cybercrime Costs the Global Economy $450 Billion." [Online] CNBC. https://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html.

7. Morgan, Steve. Cyber Crime Costs Projected to Reach $2 Trillion by 2019. [Online] Forbes, January 17, 2016. https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#6923f2ff3a91.

8. Protocol Labs. Filecoin: A Decentralized Storage Network. [https://filecoin.io/filecoin.pdf]

9. Buterin, Vitalik. Ethereum Whitepaper. [https://github.com/ethereum/wiki/wiki/White-Paper]

10. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. [https://bitcoin.org/bitcoin.pdf]

11. block.one. EOS.IO Technical White Paper. [https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md]