HEROIC
.com

Segurança Cibernética movida por Inteligência Artificial e Blockchain

Equipe HEROIC.com
Fevereiro de 2018

Resumo

A HEROIC.com está energizando o futuro da segurança cibernética com inteligência artificial e *blockchain* para proteção contra ameaças cibernéticas atuais e da próxima geração.
Como as ameaças cibernéticas estão crescendo a uma taxa exponencial, as soluções modernas de cibersegurança são reativas, desatualizadas e ineficazes. (1) A grande maioria dos dados das ameaças é controlado por grandes corporações e governos, tornando difícil e caro criar soluções de próxima geração que melhorem a proteção. Os avanços recentes na inteligência artificial baseadas na proteção sobre ameaças são promissores, mas as soluções são quase que exclusivamente usadas em grandes aplicativos corporativos, o que coloca a tecnologia fora do alcance das pessoas mais vulneráveis a ataques.

A HEROIC.com está adotando uma nova abordagem para proteção contra ameaças movida por IA. Utilizando *big data*, inteligência artificial e *blockchain*, combinados com uma plataforma P2P descentralizada de proteção contra ameaças, a Heroic.com mudará a cibersegurança como a conhecemos e disponibilizará soluções de próxima geração para todos. A HEROIC.com capacitará e incentivará desenvolvedores e empresas para criar a próxima geração de cibersegurança através do Ecossistema HEROIC.com, que inclui um intercâmbio aberto de inteligência sobre ameaças chamado HEROIC Arc Reactor™, uma plataforma unificada de gerenciamento de segurança chamada HEROIC Guardian™ e um ambiente de Pesquisa e Desenvolvimento. A motivação para a colaboração dentro desse Ecossistema será incentivada através do *blockchain* e do uso de criptomoedas da Heroic.com, a HRO (pronuncia-se *hiro*).

Este documento apresenta várias tecnologias novas e exclusivas específicas para o Ecossistema Heroic.com, incluindo os protocolos Threat Mining™, Cyberlytics™ e oProof-of-Threat™. Antecipamos milhares de aplicativos em potencial para os quais os dados fornecidos podem ser usados. Um ecossistema de cibersegurança aberto, movido a *blockchain*, abrirá a enorme oportunidade de proteção contra ameaças de próxima geração, eliminará o atrito e os custos gerados por intermediários e proporcionará um mundo mais seguro.

Acreditamos que a combinação de dados sobre ameaças cibernéticas, integrados à inteligência artificial e ao *blockchain*, é o futuro da segurança cibernética movida por IA. O ecossistema HEROIC.com e o *token* HRO se tornarão um novo padrão usado em toda a indústria de segurança cibernética para garantir globalmente segurança, privacidade e confiança.

Aviso: Este documento é apenas para fins informativos e não constitui uma oferta ou solicitação para vender ações ou títulos da HEROIC.com ou qualquer empresa ou organização relacionada ou associada. Qualquer oferta ou solicitação será feita apenas por meio de um memorando de oferta confidencial e de acordo com os termos de todos os valores mobiliários aplicáveis e outras leis.

Aviso: Este documento é apenas para fins informativos e não constitui uma oferta ou solicitação para vender ações ou títulos em HEROIC.com ou qualquer empresa ou organização relacionada ou associada. Qualquer oferta ou solicitação será feita apenas por meio de um memorando de oferta confidencial e de acordo com os termos de todos os títulos aplicáveis e outras leis.

Índice

O Problema das Atuais Soluções de Cibersegurança

Grande parte da nossa vida depende da confiança na tecnologia: a confiança em que é seguro avançar quando a luz fica verde; em que é seguro colocar nosso dinheiro em um banco ou uma loja on-line. Quase tudo que usamos todos os dias depende de tecnologia, desde despertadores e torradeiras até brinquedos e carros infantis. Estima-se que até 2020 haverá mais de 30 bilhões de dispositivos conectados à Internet. (2)

Combinado ao aumento exponencial da tecnologia, o mundo está vendo um aumento similar de ataques maliciosos. (3) Na medida em que os dispositivos vão ficando mais inteligentes e interconectados, estão sendo introduzidos riscos significativos para a privacidade e segurança. Nossos dispositivos não só são vulneráveis a ataques; os detalhes mais importantes de nossas vidas são armazenados nesses dispositivos e nos serviços de nuvem vinculados. Esses detalhes vão desde nossos registros médicos até nossas informações bancárias e comunicações privadas com familiares e amigos.

Informações privadas nas mãos erradas podem ter consequências catastróficas. A CEO da IBM, Ginny Rometty, disse: “Acreditamos que os dados são o fenômeno do nosso tempo. É o novo recurso natural do mundo. [...] o cibercrime, por definição, é a maior ameaça para todas as profissões, todos os setores, todas as empresas do mundo”. (4)

O nível universal de insegurança e os custos reais associados a violações de dados e crimes cibernéticos são surpreendentes: “72% das empresas maiores relataram um incidente cibernético no ano passado e quase metade (47%) de todas as empresas dos EUA tiveram dois ou mais”. (5) Em 2016, mais de três bilhões de registros pessoais foram roubados e vazaram para a Dark Web e mais de 100 milhões de americanos tiveram seus registros médicos roubados. (6) Quase todas as pessoas no mundo que estão conectadas à Internet foram afetadas por uma ou mais violações de dados.

O aumento contínuo das ameaças não mostra nenhum sinal de que a velocidade diminuirá em breve. Em um artigo da Forbes, Steve Morgan da CSO Online declarou: “De 2013 a 2015 os custos do cibercrime quadruplicaram, e parece que haverá outra quadruplicação de 2015 a 2019. A Juniper Research previu recentemente que a rápida digitalização das vidas dos consumidores e dos registros corporativos aumentará o custo das violações de dados para US $ 2,1 trilhões globalmente até 2019, aumentando em quase quatro vezes o custo estimado das violações de 2015”. (7)

As soluções atuais não conseguem acompanhar o número crescente e a inteligência das ameaças que atacam nossos sistemas. Os sistemas de detecção sobre ameaças baseados em assinatura comumente usados atualmente não detectam ameaças novas e inéditas. Embora seja eficaz se o vetor sobre ameaças for conhecido e as assinaturas forem totalmente atualizadas,

essas soluções reativas não poderão nos proteger contra a próxima geração de ataques inteligentes. De carros autônomos a implantes médicos e inteligência artificial geral (IA), o futuro dos *malwares* e sistemas inteligentes começará a atacar a tecnologia à qual confiamos nossas vidas e as vidas de nossos entes queridos. Nos últimos anos, avanços significativos foram feitos com a proteção contra ameaças movida por IA, mas essa tecnologia ainda não chegou às massas. As soluções da próxima geração são quase exclusivamente focadas na solução de problemas para a empresa, com muito pouco foco em usuários individuais, famílias ou empresas de pequeno e médio porte.

Além do foco na empresa, os dados sobre ameaças cibernéticas, que são o componente principal necessário para construir algoritmos inteligentes, são principalmente controlados e armazenados por governos e grandes corporações. O acesso a esses dados é fundamental, mas é proibitivamente caro, o que dificulta que os desenvolvedores e as pequenas organizações criem soluções de próxima geração e soluções movidas por IA.

É claro que a melhoria incremental não é suficiente para proteger contra o perigo à nossa porta. A inovação radical é imperativa... algo *HEROICO*.

2 Visão Geral do Ecossistema

Ecossistema HEROIC.com (o “Ecossistema”) é um ecossistema de segurança cibernética aberto, inteligente e impulsionado por *blockchain*, que protege contra ameaças cibernéticas atuais e de próxima geração. Os principais componentes do ecossistema são:

1) uma plataforma de inteligência sobre ameaças cibernéticas descentralizada chamada ***HEROIC Arc Reactor™*** (“Arc Reactor”);
2) um sistema unificado de gerenciamento sobre ameaças baseado em nuvem chamado ***HEROIC Guardian™*** (“Guardião”), e;
3) ***um Ambiente de Pesquisa e Desenvolvimento*** (“Ambiente P & D”) para desenvolvedores desenvolverem e testarem seus próprios algoritmos em uma plataforma segura e hospedada.

Esses três componentes principais são integrados e compreendem o ecossistema.

Trata-se de uma abordagem única para criar um ecossistema de longo prazo, sustentável e em constante evolução para proteção contra ameaças cibernéticas. Quando estiver plenamente operacional, o Ecossistema fornecerá os recursos necessários para proteção contra ameaças atuais e de próxima geração de modo inteligente.

2.1 Arc Reactor

HEROIC Arc Reactor™ é um intercâmbio descentralizado aberto de inteligência sobre ameaças de segurança cibernética, impulsionado pelo *blockchain*. O propósito do Arc Reactor é fornecer um depósito aberto de inteligência sobre ameaças cibernéticas, um acesso programático simples aos dados e um mercado eficiente para os dados.

Os provedores de dados incluem, mas não estão limitados a, mineradores sobre ameaças individuais, provedores de inteligência contra ameaças de código aberto, organizações de todos os portes e parceiros de dados. Os dados coletados passam por um processo de extração para retirar atributos relevantes que são então normalizados e salvos em um banco de dados difundido. Os dados coletados com seus atributos estão prontos para serem usados para treinar algoritmos de aprendizado de máquina que, em última instância, permitirão pontuar e classificar as amostras.

O acesso às amostras coletadas e seus atributos estará disponível de forma programática por meio de APIs e SDKs em conformidade com os formatos padrão da indústria.

O Arc Reactor se tornará mais inteligente e robusto, à medida que mais usuários, organizações e provedores de dados ingressarem no ecossistema. Esperamos que os dados fornecidos pelo Arc Reactor impulsionem muitos produtos relacionados à segurança cibernética e, eventualmente, se tornem o maior depósito mundial de inteligência sobre ameaças cibernéticas.

Um intercâmbio descentralizado e aberto sobre ameaças derrubará as barreiras de entrada ao construir soluções de segurança cibernética movidas por IA e permitirá que os dados sobre ameaças sejam distribuídos para benefício universal.

O mercado para os dados fornecidos pelo Arc Reactor é exclusivamente alimentado pelo *token* HRO e pelos contratos inteligentes relacionados com ele.

2.1 Guardião

A HEROIC Guardian™ é uma plataforma de segurança cibernética unificada e baseada na nuvem. Ela fornece uma *interface on-line* simples para usuários individuais, famílias e empresas gerenciarem todas as peças do quebra-cabeça de segurança cibernética. O Guardião utiliza os dados sobre ameaças do Arc Reactor e os combina com inteligência artificial para prever e prevenir ataques cibernéticos.

O Guardião permitirá que desenvolvedores e organizações de *software* desenvolvam integrações e aplicativos adicionais que se conectam com o Guardião e sua camada de dados. Essas integrações permitirão que os desenvolvedores cresçam e monetizem suas criações, levando a uma plataforma de segurança cibernética ainda mais robusta e holística.

O Guardião é fornecido como um serviço gratuito com integrações adicionais e serviços de terceiros fornecidos por um custo extra. Os usuários podem pagar por serviços *premium* usando *tokens* HRO ou moeda fiduciária. O Guardião também fornecerá acesso a uma carteira segura para gerenciar os *tokens* do HRO.

2.2 Ambiente de pesquisa e desenvolvimento

O Ambiente de P & D fornecerá a desenvolvedores, organizações e empresas um local central para interagir visual e programaticamente com dados históricos e em tempo real sobre ameaças fornecidos pelo Arc Reactor.

Os desenvolvedores podem pesquisar, desenvolver e testar seus próprios algoritmos em um ambiente seguro e hospedado. O ambiente também fornecerá acesso a algoritmos e software disponibilizados pela comunidade para analisar e bloquear ameaças, com a capacidade de transformar dados impressionantes e distintos em informações e inteligência acionáveis.

A HEROIC.com dedica-se a fornecer dados, ferramentas e *software* necessários para construir a próxima geração de segurança cibernética movida por IA. Ajudaremos a facilitar e incentivar o desenvolvimento de soluções de *software* de código aberto, conforme necessário, sendo a primeira delas uma proteção contra ameaças movida por IA.

O acesso a dados e recursos no Ambiente de P & D será exclusivamente através do *token* HRO.

3 Participantes do Ecossistema

3.1 Indivíduos (usuários e mineradores sobre ameaças)

Indivíduos que participam do ecossistema receberão softwares multifuncionais que incluem proteção contra ameaças movida por IA, funcionalidade de mineração sobre ameaças, uma carteira segura para *tokens* HRO e uma conexão com o ecossistema.

Os usuários não apenas poderão proteger seus dispositivos com o *software*, mas também ganharão *tokens* HRO à medida que o sistema encontrar, analisar e compartilhar dados sobre ameaças anônimas. À medida que mais usuários ingressam no ecossistema, grandes quantidades de dados podem ser analisadas pelos algoritmos de aprendizado de máquina da comunidade, o que torna todos mais seguros.

O *software* estará disponível para a maioria dos dispositivos, incluindo computadores *desktop*, *laptops*, *smartphones* e dispositivos *IoT*. O gerenciamento do *software* será feito pelo Guardião. O poder computacional, o armazenamento de dados e os dados contribuídos para o Ecossistema serão compensados com o *token* HRO e passarão por um escudo de anonimato que retira qualquer informação de identificação pessoal (PII).

Mineradores sobre ameaças são aqueles indivíduos que permitem que seus dispositivos se tornem anonimamente parte do ecossistema, formando um poderoso coletivo de dispositivos individuais e poder de computação. Os dispositivos que participam ativamente da mineração sobre ameaças recebem uma compensação expressa em HROs por informações e inteligência extraídas.

A HEROIC.com facilitará a participação dos usuários sem precisar entender como a tecnologia subjacente funciona e fornecerá cursos *on-line* como parte da plataforma Guardião.

3.2 Desenvolvedores

Os desenvolvedores terão acesso franqueado à totalidade do ecossistema. O principal benefício para os desenvolvedores é o Ambiente de P & D, que oferece a oportunidade de pesquisar, desenvolver, testar e distribuir seus próprios *softwares* e algoritmos.

Os desenvolvedores serão recompensados por suas criações, que podem incluir algoritmos inteligentes, ferramentas de *software* e sistemas completos de *software*. A compensação do ecossistema é feita exclusivamente através do *token* HRO.

Benefícios adicionais inclusos:

- Acesso a um dos maiores depósitos de inteligência de ameaças cibernéticas de código aberto
- Uma comunidade robusta de desenvolvedores focados em segurança cibernética e inteligência artificial
- Capacidade de pesquisar visual e programaticamente, criar e testar algoritmos proprietários usando dados históricos e em tempo real sobre ameaças

- Fluxos de receita legítimos para desenvolvedores e especialistas em segurança
- Compensação via *token* HRO para participação de dados e algoritmos mais eficazes de bloqueio sobre ameaças
- Capacidade de baixar e usar os dados para a pesquisa e os produtos de segurança cibernética dos desenvolvedores
- Compensação pela construção de aplicações descentralizadas (Dapps) que interagem com o ecossistema.

Prevemos que o ecossistema inspirará pessoas talentosas em todos os lugares para escrever algoritmos de segurança cibernética e construir soluções para o bem maior.

3.3 Organizações

A exemplo dos desenvolvedores, as organizações também terão acesso aberto à totalidade do ecossistema para uso na proteção de seus dados, recebendo compensação pelos dados fornecidos e integrando-os a produtos e serviços de terceiros.

As organizações são uma parte importante do ecossistema, uma vez que ajudarão a contribuir com grandes quantidades de dados que protegem todo o ecossistema e fornecerão um mercado eficiente de dados sobre ameaças. As organizações poderão incluir empresas, escolas, organizações sem fins lucrativos, associações de mineração, governos e outros.

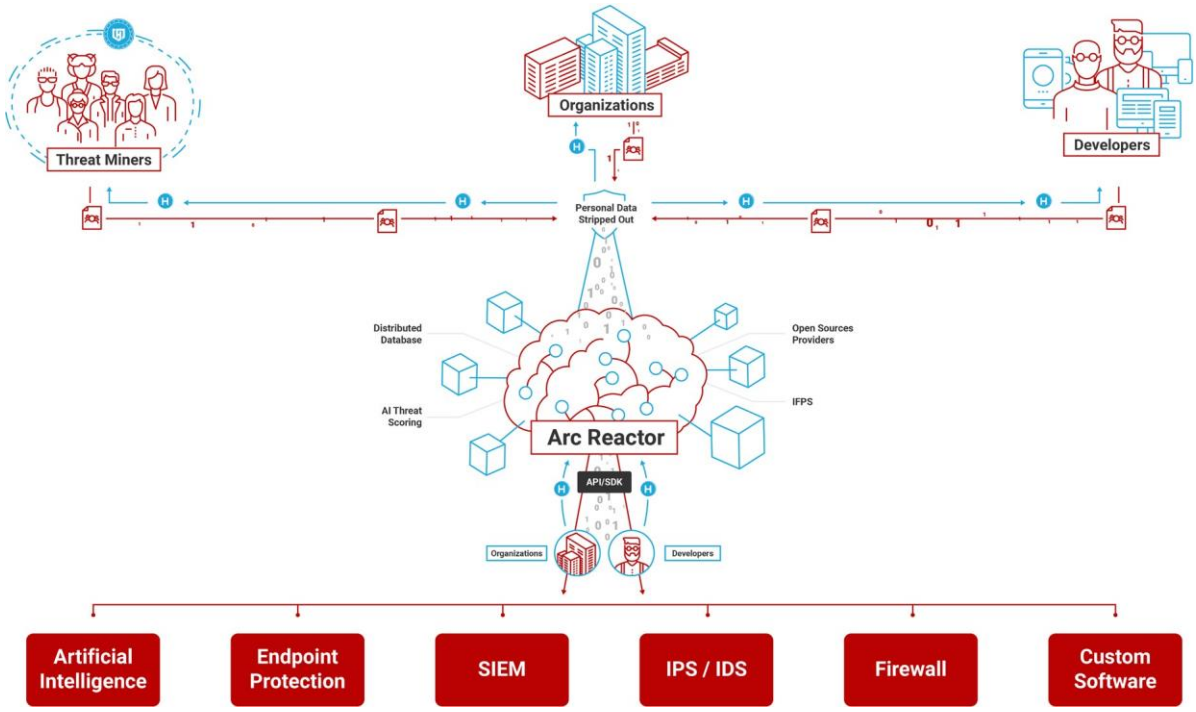
Usando métodos-padrão de distribuição da indústria, as organizações poderão consumir os dados para uso com sistemas internos de segurança cibernética e para construir seu *software* próprio.

Benefícios para as organizações incluem:

- Acesso a um dos maiores depósitos de inteligência sobre ameaças cibernéticas de código aberto
- Compensação por participação de dados e contribuições para algoritmos de bloqueio sobre ameaças
- Capacidade de baixar dados sobre ameaças para aprimorar seus próprios produtos de segurança cibernética
- Compensação pela construção de aplicações descentralizadas (Dapps) que interagem com o ecossistema.

4 Visão Geral da Tecnologia

Conforme descrito acima, o ecossistema HEROIC.com consiste em três projetos principais que se combinam para elaborar uma solução de segurança eficaz que beneficia todos os tipos de usuários, incluindo usuários individuais, desenvolvedores e organizações. Ele foi projetado para fornecer múltiplos níveis de acesso, valor e suporte, a fim de estimular a pesquisa acelerada, o desenvolvimento e a integração de tecnologias avançadas de segurança cibernética, além de garantir o acesso universal a essas tecnologias. Quanto mais o ecossistema crescer, mais forte ele será.



4.1 Arc Reactor

O Arc Reactor é uma plataforma aberta e descentralizada de inteligência sobre ameaças de segurança cibernética que supre três funções principais, que são a coleta, a transformação e a distribuição de dados sobre ameaças, para uso com inteligência artificial e sistemas de segurança cibernética. Abaixo, consideramos cada uma das três funções:

Coleta

Os dados sobre ameaças são coletados de várias fontes, incluindo mineiros sobre ameaças, fontes de ameaças de código aberto, provedores de inteligência sobre ameaças comerciais, inteligência sobre ameaças fornecida pela comunidade e compartilhamento sobre ameaças às organizações. Cada fonte participante do ecossistema é um agente autônomo, capaz de realizar essas ações com interação humana limitada.

Os participantes do ecossistema receberão agentes de *software* e acesso programático para contribuir com um fluxo constante de dados sobre ameaças. Os dados coletados passam por um escudo de anonimato para garantir que nenhuma informação de identificação pessoal seja compartilhada.

Transformação

Dados coletados sobre ameaças passam por um processo de limpeza que inclui verificação, normalização, desduplicação e enriquecimento. Esses dados limpos serão armazenados em uma rede de armazenamento disponibilizado usando IPFS e os metadados serão armazenados em um banco de dados distribuído.

Uma vez armazenados, os dados sobre ameaças passarão por processos adicionais que associam, classificam e pontuam os dados usando inteligência artificial. Esses metadados adicionais associados à amostra serão então mesclados com os metadados no banco de dados distribuído.

Distribuição

Diversos *feeds* de dados sobre ameaças serão fornecidos aos participantes do ecossistema, incluindo: detalhes do arquivo, domínio, dados de URL e IP, dados da Dark Web, COI e dados da comunidade. O acesso aos *feeds* de dados será fornecido programaticamente usando os padrões do setor por meio de APIs e SDKs. Esses padrões podem incluir YARA, STIX, TAXII, CybOX e outros.

O Arc Reactor fornecerá os grandes dados e incentivos necessários para alimentar a inteligência artificial que pode ser usada para proteger contra ameaças. Esperamos que os dados sobre ameaças sejam usados em muitos aplicativos diferentes, incluindo Endpoint Protection movida por IA, Sistemas de Prevenção de Invasão / Detecção de Invasão, Informações de Segurança e Gerenciamento de Eventos (SIEM), Identificação de *Botnets* e Identificação e Prevenção de *Phishing*.

4.2 Guardião

Várias camadas de segurança são necessárias para proteger a tecnologia de um usuário. Essas camadas incluem *software* antivírus, monitoramento de violação de dados, proteção contra roubo de identidade, gerenciamento de credenciais, *backups*, DNS e muitos outros sistemas. Na HEROIC.com, muitas vezes chamamos essas camadas de quebra-cabeças da segurança cibernética.

O Guardião é uma plataforma unificada de segurança cibernética baseada em nuvem que fornece uma *interface* simples para usuários individuais, famílias e organizações gerenciarem todas as partes do quebra-cabeça de segurança cibernética.

O Guardião fornecerá inicialmente camadas básicas do quebra-cabeça de segurança cibernética, permitindo, ao mesmo tempo, que desenvolvedores e organizações contribuam e sejam compensadas por integrações com a Guardian App Store. Os aplicativos Guardião usarão APIs de desenvolvedor para interagir com os dados do ecossistema. Essas peças combinadas unificarão e simplificarão o gerenciamento da segurança cibernética.

O Guardião combina inteligência artificial com os dados de seus aplicativos interconectados e do Arc Reactor para prever e prevenir ataques cibernéticos. Os usuários do Guardião não só se beneficiarão da inteligência geral fornecida pelo Ecossistema, mas também terão sua própria IA pessoal dedicada à proteção de seus dispositivos e serviços em nuvem. À medida que mais dados forem analisados, o sistema ficará mais inteligente e protegerá melhor de contra-ataques.

O acervo do software do Guardião consiste nas seguintes tecnologias:

- Gerenciamento de cibersegurança unificado baseado em nuvem
- Agentes de *software* e sensores de dados
- Gerenciamento de terminal
- Desenvolvedor de APIs
- App Store para integração de terceiros
- Mecanismos de IA específicos do usuário
- Gerenciamento de transação de *blockchain*

4.3 Ambiente de Pesquisa e Desenvolvimento

O Ambiente de P & D fornece acesso simples aos dados sobre ameaças do Arc Reactor, combinados com recursos robustos de pesquisa e desenvolvimento de *software*.

Os desenvolvedores podem aprender sobre inteligência artificial e segurança cibernética em nossos tutoriais e palestras. Usando essas informações, eles podem criar e testar suas próprias criações em tempo real e dados históricos em um Ambiente de Desenvolvedor Interativo (IDE). Os desenvolvedores também receberão incentivos para criar os melhores algoritmos de proteção contra ameaças e vender sua tecnologia no mercado em troca de HROs.

A plataforma de P & D capacitará uma comunidade de desenvolvedores e pesquisadores com o conhecimento e os recursos necessários para construir a próxima geração de proteção contra ameaças.

O ambiente de P & D consiste nas seguintes tecnologias:

- Acesso a dados históricos sobre ameaças
- Desenvolvedor de APIs
- Caixa de proteção para teste de *software*
- Ferramentas de *software*
- Comunidade de IA e inteligência de cibersegurança
- Mercado movido a HRO
- Gerenciamento de transações de *blockchain*

4.4 Outras tecnologias

4.4.1 *Software* do agente

O *software* do agente pode ser instalado em dispositivos individuais e fornece uma variedade de funções, incluindo mineração de ameaças, conexões de ecossistema, proteção de terminal, uma carteira HRO segura e gerenciamento simples do sistema.

O *software* do agente estará disponível para vários dispositivos, incluindo *desktops*, *laptops*, telefones celulares e dispositivos IoT. Espera-se que o *software* do agente seja desenvolvido para todos os sistemas operacionais populares.

Cada agente individual monitorará ativamente as ações e alterações de arquivos, o tráfego do ecossistema, o comportamento do usuário e as propriedades do arquivo. Os agentes poderão identificar anomalias e ameaças independentemente, validando-as e tomando as medidas apropriadas. Esse monitoramento garantirá a proteção do usuário, bem como de seus dados.

A comunicação dentro do ecossistema será realizada entre os agentes, o Arc Reactor e o *blockchain*, a fim de caracterizar as ameaças validadas, aumentar a inteligência do sistema e providenciar a compensação das ameaças extraídas. Essa comunicação também ajudará na identificação e validação de ameaças e garantirá a transmissão de ataques ativos em tempo real.

Os dados sobre ameaças verificadas serão anonimizados e enviados ao ecossistema para ajudar outros sistemas a evitar ameaças futuras e para que os desenvolvedores criem seus algoritmos de proteção contra ameaças.

Quando estiver plenamente desenvolvido, o *software* do agente poderá atuar como principal proteção de *endpoint* do dispositivo, para identificar e bloquear ameaças, além de fornecer poder de processamento e armazenamento ao ecossistema para monitoramento e identificação remotos de ameaças.

4.4.2 Inteligência Artificial (Cyberlytics®)

A HEROIC.com usa “Inteligência Artificial” como um termo geral para descrever os muitos sistemas e processos inteligentes que serão usados dentro do ecossistema.

A Inteligência Artificial na cibersegurança engloba muitos campos diferentes de estudo, incluindo matemática, aprendizado de máquina, redes neurais, reconhecimento de padrões, identificação de anomalias e muito mais.

O Cyberlytics® é o mecanismo inteligente baseado em IA da HEROIC.com, usado para prever e prevenir ataques cibernéticos antes que eles aconteçam. O mecanismo Cyberlytics analisa uma enorme quantidade de dados complexos do Arc Reactor sobre ameaças para criar poderosos *insights* que são usados para proteger automaticamente sua tecnologia, seus dados e, por fim, você.

4.4.3 *Software* do *blockchain*

A HEROIC.com usa contratos inteligentes da Ethereum para transações que facilitam pagamentos diretos entre usuários, organizações e desenvolvedores de *software*. Usando um livro-caixa seguro baseado em *blockchain*, a HEROIC.com fornece a capacidade de adquirir, manter e transferir os HROs. Incentivaremos e recompensaremos continuamente os usuários que contribuem para o ecossistema, inclusive fazendo e recebendo pagamentos para distribuição e uso de dados sobre ameaças.

Nosso algoritmo de consenso é um *proof-of-work* baseado no protocolo de *proof-of-work* da Ethereum, que acabará se convertendo no novo protocolo Proof-of-Threat™ da HEROIC.com.

4.4.4 Proof-of-Threat™

O novo protocolo Proof-of-Threat™ da HEROIC.com será eventualmente usado como o principal método para quantificar o trabalho concluído de cada nó e fornecerá uma pontuação para cada amostra de ameaça individual. Em vez de desperdiçar energia e recursos preciosos para computar *hashes*, o protocolo Proof of Threat permitirá que as mineradoras contribuam com seus recursos de computação para a análise e pontuação sobre ameaças potenciais e sejam proporcionalmente compensadas por esse trabalho.

A pontuação de ameaças fornece um valor numérico para cada ameaça individual. A pontuação indica a probabilidade de a amostra ser uma ameaça. Quanto maior a pontuação, maior a probabilidade de ser uma ameaça.

A pontuação das amostras é benéfica, pois proporciona aos sistemas maior controle sobre o bloqueio ou desbloqueio da ameaça, em vez de fornecer um valor binário simples sobre se algo é ou não uma ameaça.

Uma pontuação de ameaça é baseada em vários fatores e usa uma média aritmética ponderada para produzir uma pontuação de zero a 100. A HEROIC.com adota uma abordagem de aprendizado de máquina, inicialmente pontuando cada amostra em um nó e, em seguida, usando dados do Arc Reactor para validar a pontuação inicial e aprender com os dados.

A pontuação da Proof-of-Threat será calculada usando alguns ou todos os sistemas a seguir:

- Pré-execução
  - Mecanismos cibernéticos movidos por IA da HEROIC
  - Comparação de *hash* de artefato com ameaças conhecidas no Arc Reactor
- Pós-execução
  - Análise do artefato heurístico que observa comportamento ou características de um arquivo ou processo que pode indicar que é suspeito.
  - Análise da Caixa de Proteção

O protocolo Proof-of-Threat™ e o mecanismo de pontuação de ameaças serão de código aberto e estarão disponíveis para todos. Um *white paper* mais abrangente sobre a implementação inicial do Proof-of-Threat™ será lançado em um momento futuro.

4.4.5 Preço dos dados (algorismos de precificação dinâmica)

O preço dos dados de ameaça é um dos aspectos mais importantes do ecossistema, pois o sistema deve motivar os usuários a contribuir com dados por meio de sua estrutura de preços, ao mesmo tempo que não afasta os consumidores dos dados devido ao alto custo dos mesmos.

Em vez de fornecer um sistema de preços bidirecional que agregue conflito e complexidade desnecessários aos usuários, estamos construindo um algoritmo de precificação automatizado em tempo real que motiva os provedores de dados, maximizando a lucratividade, motivando os consumidores dos dados sobre ameaças e propondo preços altamente competitivos. Esse sistema é semelhante ao que o Uber usa para propor preços aos seus passageiros e motoristas, já que não há necessidade de escolha do usuário ou transparência explícita em como os preços são determinados.

O algoritmo fornece preços dinâmicos com base na oferta e demanda dos dados fornecidos. Leva em consideração características como idade e tamanho dos dados, seu tipo e sua importância potencial, o tamanho total do pedido, pontuação de ameaça e outras condições de mercado.

À medida que recebermos o *feedback* dos usuários do Ecossistema e nosso entendimento do valor dos dados aumentar, atualizaremos continuamente o algoritmo e integraremos o aprendizado de máquina para proporcionar uma praça de mercado cada vez mais eficiente.

A seguir, um exemplo da noção matemática atual que será implementada.

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

F = total de ganhos mensais para cada minerador de ameaça
M = Tipo de dados 1 (valor A%) (conforme determinado por outros fatores)
N = Tipo de dados 2 (avaliado em B%) (determinado por outros fatores)
P = Tipo de dados 3 (valorado em C%) (conforme determinado por outros fatores)

X = renda auferida dos consumidores de dados naquele mês

5 Informações sobre o Token

5.1 *Token* HRO

Como parte do desenvolvimento do ecossistema HEROIC.com, estamos introduzindo o *token* HRO (pronuncia-se *hiro*), que será usado como uma forma de autorização, incentivo e liquidação entre os participantes do ecossistema e para outros serviços relacionados.

Uma oferta fixa de HROs será criada como parte da venda de *tokens*, com contratos inteligentes apropriados e um *ledger* baseado em *blockchain* que seguirá o padrão ERC20. O *ledger* fornecerá um método seguro para os detentores de HROs manterem e transferirem HROs para outros usuários.

Embora a HEROIC.com pretenda desenvolver o *software* inicial e os contratos inteligentes que alimentam o ecossistema, esperamos que o HRO seja um novo padrão usado em todo o ecossistema de segurança cibernética e em outros setores.

5.2 Incentivos e benefícios do *token*

O ecossistema foi projetado para fornecer múltiplos níveis de acesso, valor e apoio, a fim de estimular pesquisas aceleradas, desenvolvimento e integração de tecnologias avançadas de segurança cibernética e assegurar a disponibilidade dessas tecnologias para todos. Os incentivos serão gerenciados por meio do uso dos *tokens* HRO, com o ecossistema sendo multitransacional, permitindo compras e pagamentos entre qualquer combinação de participantes do HEROIC.com, incluindo usuários finais, desenvolvedores e organizações.

5.3 Mercado do *token*

HEROIC.com está construindo um mercado robusto para dados sobre ameaças, alimentado pelo *token* HRO. Os HROs poderão ser adquiridos com Bitcoin (BTC), Ethereum (ETH) e outras criptomoedas populares ou com moeda fiduciária.

Os usuários que possuem HROs poderão usar seus *tokens* para adquirir serviços existentes e futuros diretamente do HEROIC.com e de outros parceiros do ecossistema.

O *token* estará disponível em mercados de criptografia selecionados. Os participantes do ecossistema receberão, cada um, uma carteira segura com a qual poderão gerenciar seus *tokens* HRO.

5.4 Fundo de crescimento do usuário

Um fundo de crescimento de usuários será implementado para incentivar os usuários a participarem das várias vertentes do ecossistema. A HEROIC.com também incentivará e ajudará a facilitar o desenvolvimento de serviços adicionais relacionados à segurança cibernética que poderão ser trocados por *tokens HRO*.

6 Privacidade & Segurança

Um projeto da magnitude e importância do Ecossistema da HEROIC.com torna necessária uma declaração sobre a importância e a aplicação de privacidade e segurança.

A privacidade é de suma importância para nós. Faremos o possível para manter a conformidade com as regulamentações relacionadas, incluindo a Prevenção de Perda de Dados (DLP), as diretrizes do NIST, os requisitos do GRDP e outras práticas recomendadas de segurança cibernética. Assim sendo, ferramentas, processos e sistemas de proteção de dados são fundamentais para garantir a privacidade dos clientes da HEROIC.com, e quaisquer dados armazenados são mantidos.

A HEROIC.com se esforçará para empregar as tecnologias e os padrões de segurança cibernética mais recentes e continuará a evoluir e ser transparente sobre a tecnologia que usa. As políticas da HEROIC.com são projetadas para garantir que os dados armazenados não sejam disponibilizados para pessoas ou organizações não autorizadas.

Como parte de nosso plano de segurança cibernética, manteremos um programa de recompensas de *bugs* para todos os ângulos de nossa arquitetura, com recompensas denominadas de *tokens* HRO. É importante notar que nosso objetivo é chegar a hospedar todas os recursos do ecossistema na *Zero-Knowledge Architecture*.

Visando impor padrões éticos aos usuários, poderá ter negado permanentemente o acesso e perder o acesso aos seus *tokens* HRO qualquer participante ou usuário que propositalmente cause danos ao ecossistema, às plataformas ou aos aplicativos ou que use os dados para fins não éticos.

7 Outras Tecnologias da HEROIC.com

HEROIC.com é um derivado de uma empresa duas vezes Inc. 500 especializada em segurança cibernética e desenvolvimento de software, e que foi fundada com a missão de proteger de forma inteligente as informações do mundo. Com essa missão, a HEROIC.com tem estado ativamente envolvida no desenvolvimento de vários produtos de segurança cibernética. Os produtos a seguir estão disponíveis atualmente e estão sendo usados por grandes organizações.

7.1 HEROIC DarkHive™

A HEROIC DarkHive é uma das maiores coleções mundiais de credenciais de usuário vazadas e comprometidas. HEROIC.com usa tecnologia inteligente e analistas de segurança cibernética para vasculhar a *deep and dark web* por *hacks*, vazamentos e qualquer outra fonte de dados comprometidos.

O DarkHive inclui tanto dados detalhados quanto dados resumidos, para uso em empresas ao redor do mundo. O DarkHive é o grande depósito de dados que alimenta o EPIC (veja abaixo).

7.2 HEROIC EPIC™

O HEROIC EPIC ajuda a descobrir, remediar e impedir o uso de credenciais de *login* roubadas encontradas em violações e vazamentos de dados de terceiros.

Em 2016, mais de 3,3 bilhões de registros, incluindo endereços de e-mail, nomes de usuários e senhas de mais de 1.700 violações de dados, foram divulgados na Dark Web. Uma vez tornados públicos, os *hackers* e outras partes podem obter e usar esses registros para forçar sua entrada nos sistemas e ecossistemas das organizações, para realizar ataques direcionados. O EPIC descobre vulnerabilidades e evita ataques obtendo os mesmos bancos de dados vazados da Dark Web e notificando as organizações se os dados de seus funcionários ou clientes tiverem sido comprometidos. Isso dá aos profissionais de segurança a oportunidade de corrigir *log-ins* roubados antes de serem usados contra seus proprietários.

8 Trabalho Futuro

A equipe do HEROIC.com acredita que, para cumprir nossa missão de fornecer segurança cibernética de última geração a todos, o ritmo atual de desenvolvimento é insuficiente para superar a taxa de ameaças cibernéticas e, portanto, requer expansão significativa e desenvolvimento acelerado.

Como afirmado no Resumo, esperamos que existam literalmente milhares de aplicativos potenciais para os quais os dados fornecidos pelo ecossistema HEROIC.com possam ser usados. Não pretendemos construir a grande maioria desses aplicativos, mas facilitar e motivar outras pessoas no ecossistema a construir esses sistemas.

Os fundos arrecadados com a venda simbólica serão aplicados aos projetos listados neste documento, com a prioridade inicial de completar o ecossistema HEROIC.com, a fim de fornecer aos usuários uma plataforma descentralizada para gerenciar todos os aspectos de suas necessidades de segurança cibernética.

Esse documento estabelece um caminho claro e coeso para a construção do ecossistema. No entanto, também consideramos que é um ponto de partida para pesquisas futuras sobre *software* de segurança cibernética movida por IA.

A pesquisa ativa é contínua e novas versões deste artigo aparecerão na HEROIC.com. Para comentários e sugestões, entre em contato conosco pelo e-mail contact@HEROIC.com.

8.1 Trabalho em andamento

Os tópicos a seguir representam o trabalho relevante em andamento que deve trazer benefícios significativos ao ecossistema HEROIC.com.

- Uma especificação de protocolo de prova de ameaça totalmente implementável
- Pesquisa em soluções emergentes de armazenamento descentralizado
- Estimativas detalhadas de desempenho e *benchmarks* para o ecossistema HEROIC.com e seus componentes
- Mecanismos de algoritmos de aprendizado para uma praça de mercado mais eficiente de dados sobre ameaças
- Análise teórica do jogo dos incentivos do HEROIC.com
- Transações de milissegundos via ecossistemas fora da cadeia semelhantes aos https://lightning.ecosystem relacionados ao Bitcoin ou Ethereum Raiden https://raiden.ecosystem/
- Integração com outros *blockchains*
- Penalidades para participantes ou usuários que propositalmente causem danos ao ecossistema ou a qualquer aplicativo, ou que usem os dados para fins antiéticos
- Zero-Knowledge Architecture [Arquitetura Conhecimento Zero]

9 Agradecimentos

Este trabalho é resultado do esforço concentrado de vários indivíduos da equipe da HEROIC.com e não teria sido possível sem a ajuda, os comentários e a revisão dos colaboradores e consultores da HEROIC.com. Chad Bennett é o arquiteto original do ecossistema HEROIC.com. David McDonald e ele escreveram esse *white paper* em colaboração com o restante da equipe, que forneceu contribuições, comentários, revisão e diálogo úteis. Tammy Bennett ajudou a melhorar a estrutura e a redação do documento, enquanto Wyatt Semanek criou as ilustrações e finalizou o trabalho. Múltiplos *white papers* relacionados à criptografia foram consultados na preparação deste trabalho e são mencionados nas referências (8), (9), (10) e (11). Agradecemos também a todos os nossos colaboradores e consultores pelo diálogo e suporte úteis.

10 Anexo

Segurança cibernética - uma breve história

Glossário

Movido por IA: *Software* que usa inteligência artificial ou algoritmos de aprendizado de máquina, em vez de humanos, para tornar o *software* mais inteligente.

Algoritmo: um conjunto de regras para resolver um problema em um número finito de etapas, como para encontrar o maior divisor comum.

Inteligência Artificial: Teoria e desenvolvimento de sistemas computacionais capazes de executar tarefas que normalmente requerem inteligência humana, como percepção visual, reconhecimento de fala, tomada de decisão e tradução entre idiomas.

***Big Data*:** Conjuntos de dados extremamente grandes que podem ser analisados computacionalmente para revelar padrões, tendências e associações, especialmente relacionadas ao comportamento e interações humanas.

***Blockchain*:** Consulte https://HEROIC.com/blockchain-overview

Criptomoeda: Uma moeda digital na qual as técnicas de criptografia são usadas para regular a geração de unidades monetárias e verificar a transferência de fundos, operando independentemente de um banco central ou autoridade.

Cibersegurança: o conjunto de tecnologias, processos e práticas projetados para proteger redes, computadores, programas e dados contra ataques, danos ou acesso não autorizado.

Data Mining: o processo de descobrir padrões e relacionamentos interessantes e úteis em grandes quantidades de dados.

Descentralizar: Dispersar (algo) de uma área de concentração; para criar algo sem limitar seu controle ou usar para um pequeno grupo.

Democratizado: Tornar acessível e aberto a todos. O poder é investido nas pessoas e exercido diretamente por elas.

Moeda fiduciária: Moeda que um governo declarou ter curso legal, mas que não é apoiada por uma mercadoria física. O valor da moeda fiduciária deriva da relação entre oferta e demanda, e não do valor do material de que o dinheiro é feito. Exemplos de moeda fiduciária incluem o dólar americano, euro, libra esterlina etc.

HEROIC Arc Reactor: A plataforma unificada da HEROIC.com para gerenciamento de ameaças, projetada para reunir a inteligência e os dados do mundo da segurança cibernética.

Ecossistema da HEROIC.com: O mais novo sistema ou rede de interconexão e interação de elementos, para ajudar a proteger o mundo contra ameaças cibernéticas tão rapidamente quanto são criadas ou mais rapidamente do que são criadas. O sistema empregará três novas plataformas para criar soluções de segurança cibernética rápidas, atualizadas e proativas para todos.

Guardião HEROIC: Uma plataforma unificada baseada em nuvem criada pela HEROIC.com para ajudar a proteger os usuários contra ameaças cibernéticas, usando inteligência artificial.

Machine Learning: A capacidade dos computadores aprenderem sem serem programados. Fazer previsões sobre dados.

Minerador de ameaças: Usuário do *software* de mineração de ameaças da HEROIC que pesquisam, validam e distribuem ameaças à rede.

Proteção de Ameaças: um serviço ou sistema que ajuda a proteger você ou sua empresa contra problemas ou ataques mal-intencionados.

Zero-Knowledge Architecture: Arquitetura de *software* em que o armazenamento de dados em sistemas é criptografado com chaves públicas e privadas de forma que o provedor de armazenamento não tenha acesso para descriptografar ou exibir os dados.

11 Citações

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] 24 de Outubro de 2017. https://www. visioncritical.com/internet-of-things-stats/.

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

4. ***Rometty, G. IBM Security Summit. . [Online] 4 de Maio de 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]