AIを悪用したサイバー攻撃とEDRは本当に活用されていか？

ウィズセキュア株式会社
サイバーセキュリティ技術本部
本部長　島田秋雄
akio.shimada@withsecure.com

akiio.shimada@withsecure.com

INTERNAL

本セッションの概要

1. **AIを悪用したサイバー攻撃**
   - Salesforce に関連するSalesforce 環境に対する情報漏えい対策 - セキュリティコンサルティング事例のご紹介

2. **EDRは本当に活用されているか？**

3. **クラウド環境を安全に活用するために WithSecureクラウドセキュリティ診断サービス (弊社の宣伝)**
   - WithSecure EDR, Elevate to WithSecure, Co-Monitoringのご紹介
   - Salesforce に関連するSalesforce 環境に対する情報漏えい対策 - セキュリティコンサルティング事例のご紹介
   - Salesforce 環境へのマルウェア対策
   - Salesforce 環境へのマルウェア対策の国内ユーザ様 採用事例

WithSecure 会社概要

ウィズセキュアについて

■ 1988年創業。1999年、NASDAQ OMX, Helsinkiに上場

- サイバーセキュリティ業界をリードする製品やサービスを開発・提供
- ２００人以上のホワイトハッカーを擁するセキュリティコンサルタントチームは、診断実績、ハッキングコンテスト、講演などを世界的に高い評価を得ています
- 日本法人は1999年に設立。 多数のセキュリティコンサルティングサービスやセキュリティ製品を販売しています

基本データ

WithSecure Corporation

- 会 長　　リスト・シラスマ
- 社長兼CEO　ユハニ・ヒンティッカ
- 所在地　　ヘルシンキ , フィンランド

ウィズセキュア株式会社

- 代表者　　ジョン・デューリー | 日本担当VP
- 所在地　　東京都港区
- 拠 点　　東京/大阪

売上 (2022年)
134.7M ユーロ

世界の従業員数
1,300 名

販売パートナー数
7,000+ 社

サイバーセキュリティサービス- 概要

30

30年以上の
サイバーセキュリティ
領域での経験と実績

7,000社以上の
パートナーを
通じて販売

200人以上の
ホワイト
ハッカー

世界100以上の
国々でビジネスを
展開

インターポールなど
70以上の業界
機関との協業

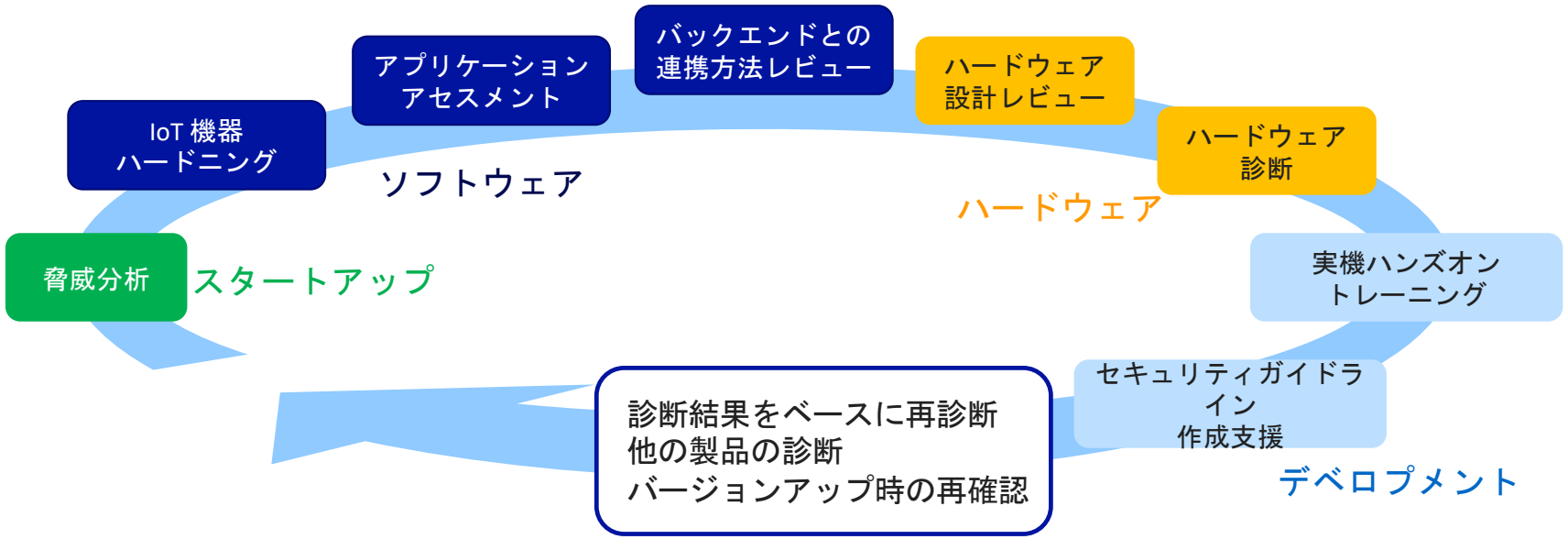
ヨーロッパのサイバー
犯罪への捜査協力実施

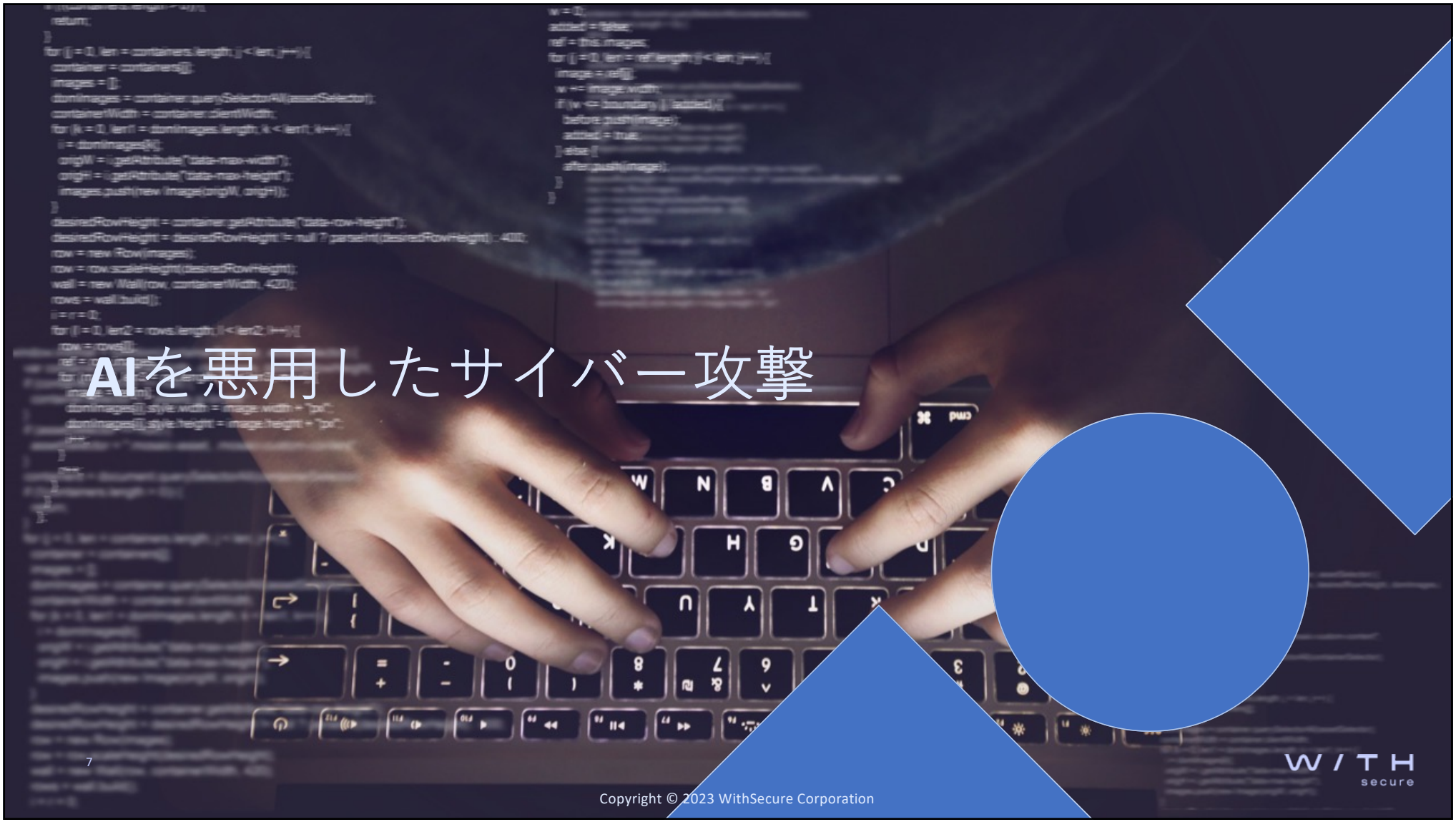
NASDAQ OMX Helsinki
に上場
(1999年)

創業以来、
セキュリティ技術の
研究・開発に注力

IoT機器からバックエンドインフラまでの総合診断

- 脅威分析を経て次の様々なステップへ進み、セキュリティ問題を可視化できます
  - 攻撃手法は巧妙化・複雑化するため繰り返し実施することで多層的・複合的な推奨が可能になります





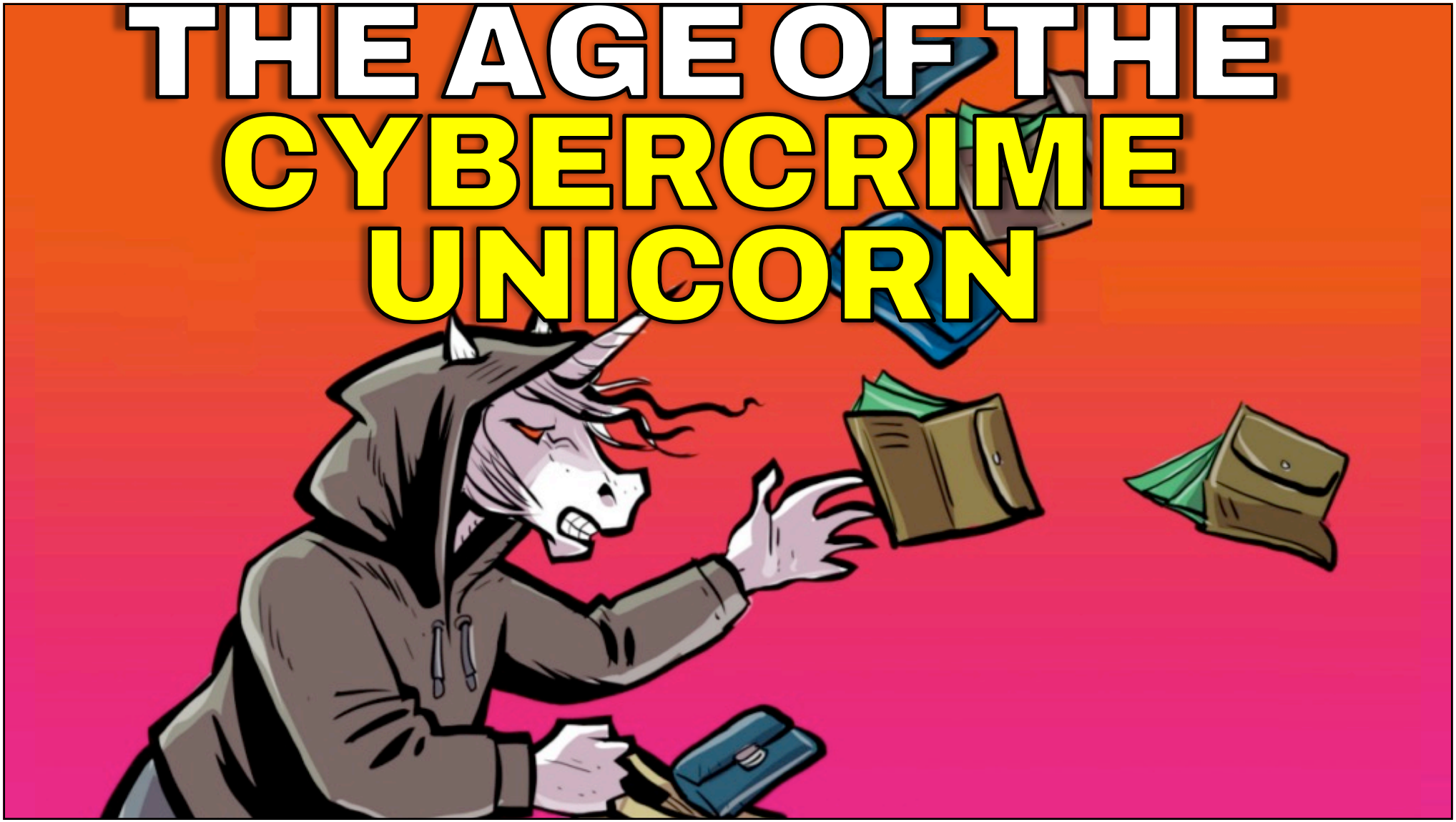

WITH secure
FIGHTING
CYBER CRIME
Mikko
Hypponen
WithSecure
@mikko

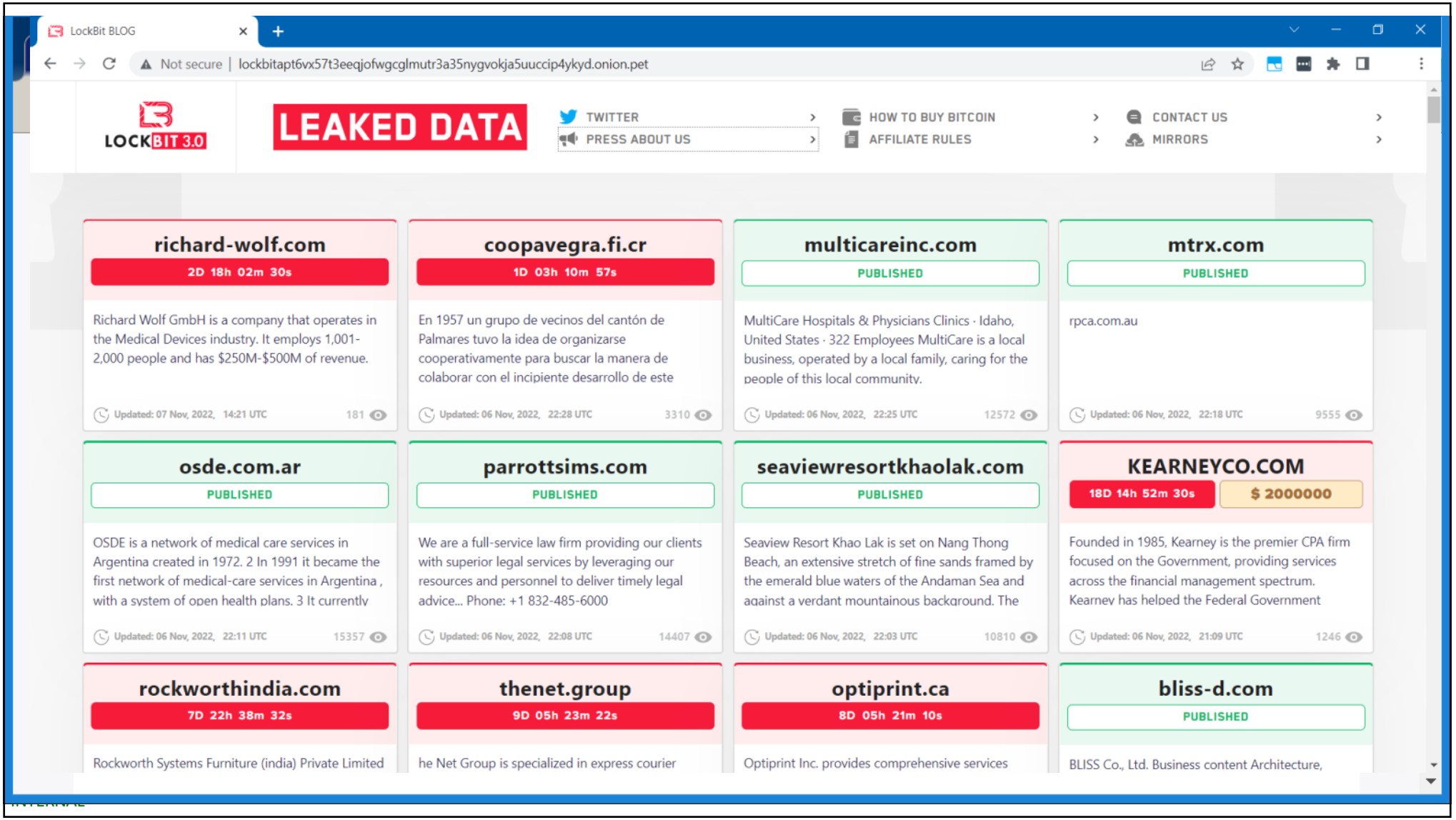

Technology
Revolutions
W/TH
secure


Threat Landscape
WITH secure

Visualization of the top malware variants found in honeypots

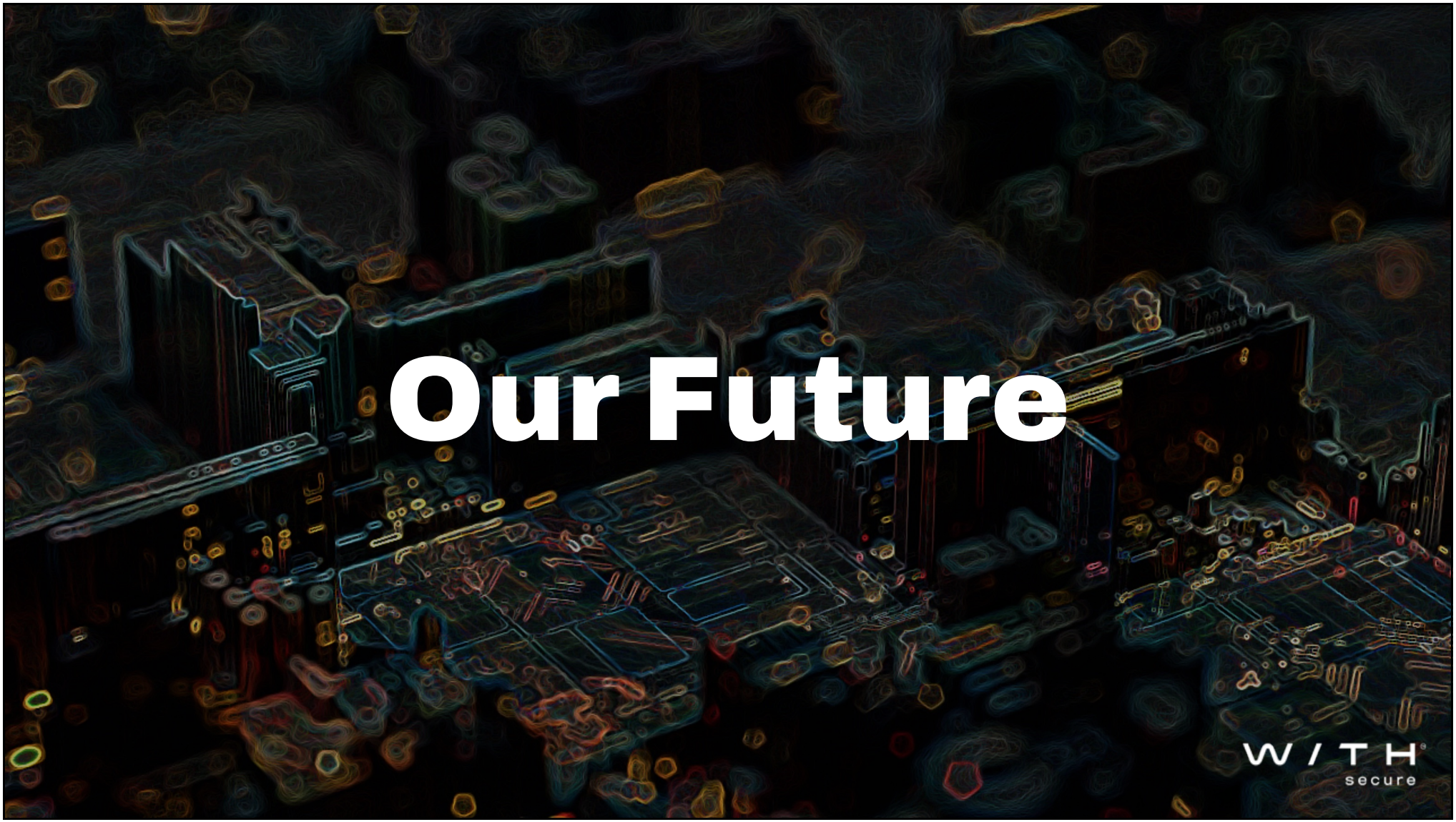
THE AGE OF THE CYBERCRIME UNICORN

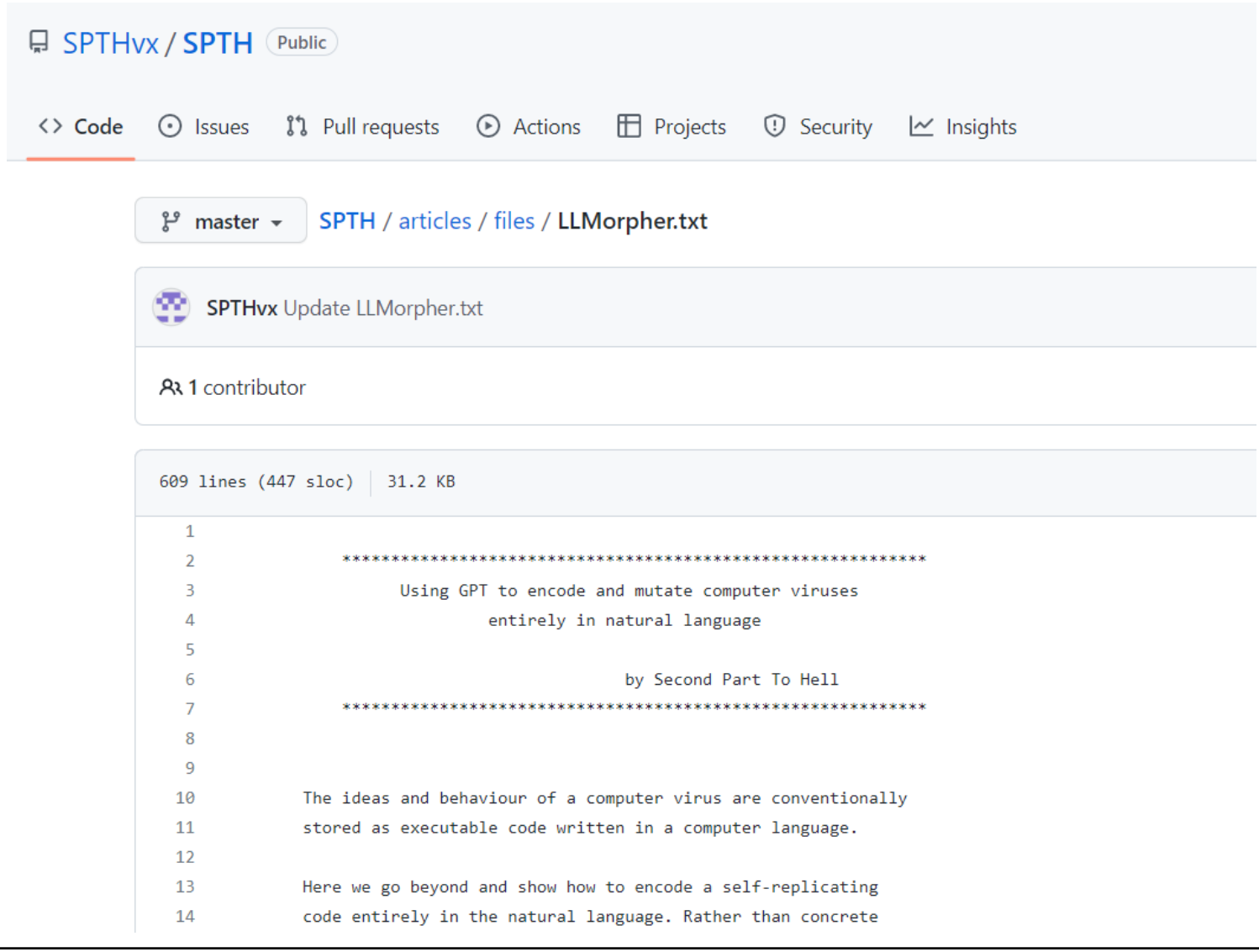


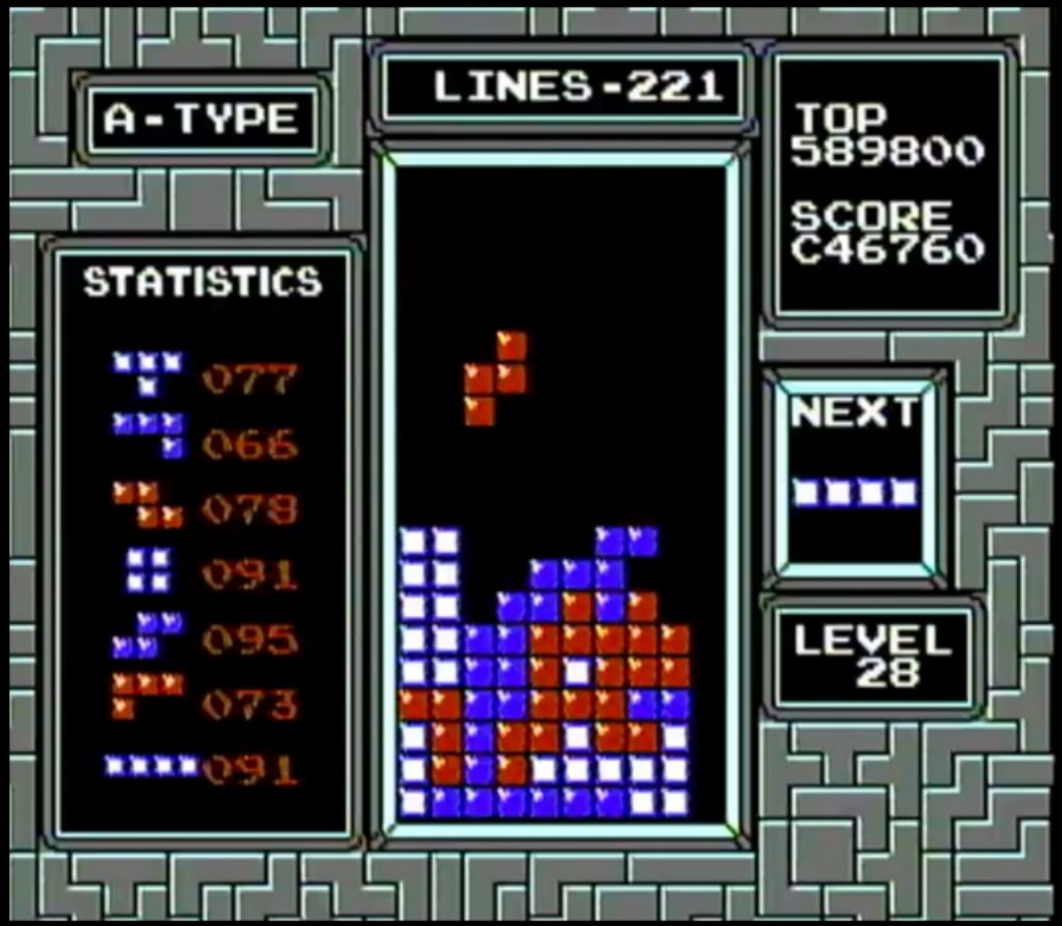

LockBit BLOG
Not secure | lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion.pet
LOCKBIT 3.0
LEAKED DATA
TWITTER
PRESS ABOUT US
HOW TO BUY BITCOIN
AFFILIATE RULES
CONTACT US
MIRRORS
richard-wolf.com
2D 18h 02m 30s
Richard Wolf GmbH is a company that operates in the Medical Devices industry. It employs 1,001-2,000 people and has $250M-$500M of revenue.
Updated: 07 Nov, 2022, 14:21 UTC
181
coopavegra.fi.cr
1D 03h 10m 57s
En 1957 un grupo de vecinos del cantón de Palmares tuvo la idea de organizarse cooperativamente para buscar la manera de colaborar con el incipiente desarrollo de este
Updated: 06 Nov, 2022, 22:28 UTC
3310
multicareinc.com
PUBLISHED
MultiCare Hospitals & Physicians Clinics · Idaho, United States · 322 Employees MultiCare is a local business, operated by a local family, caring for the people of this local community.
Updated: 06 Nov, 2022, 22:25 UTC
12572
mtrx.com
PUBLISHED
rpca.com.au
Updated: 06 Nov, 2022, 22:18 UTC
9555
osde.com.ar
PUBLISHED
OSDE is a network of medical care services in Argentina created in 1972. 2 In 1991 it became the first network of medical-care services in Argentina , with a system of open health plans. 3 It currently
Updated: 06 Nov, 2022, 22:11 UTC
15357
parrottsims.com
PUBLISHED
We are a full-service law firm providing our clients with superior legal services by leveraging our resources and personnel to deliver timely legal advice... Phone: +1 832-485-6000
Updated: 06 Nov, 2022, 22:08 UTC
14407
seaviewresortkhaolak.com
PUBLISHED
Seaview Resort Khao Lak is set on Nang Thong Beach, an extensive stretch of fine sands framed by the emerald blue waters of the Andaman Sea and against a verdant mountainous background. The
Updated: 06 Nov, 2022, 22:03 UTC
10810
KEARNEYCO.COM
18D 14h 52m 30s
$ 2000000
Founded in 1985, Kearney is the premier CPA firm focused on the Government, providing services across the financial management spectrum. Kearney has helped the Federal Government
Updated: 06 Nov, 2022, 21:09 UTC
1246
rockworthindia.com
7D 22h 38m 32s
Rockworth Systems Furniture (india) Private Limited
thenet.group
9D 05h 23m 22s
he Net Group is specialized in express courier
optiprint.ca
8D 05h 21m 10s
Optiprint Inc. provides comprehensive services
bliss-d.com
PUBLISHED
BLISS Co., Ltd. Business content Architecture,


Losing Trust


Complexity is the enemy of Security
WITH secure


Our Future
WITH
secure


SPTHvx / SPTH
Public
Code
Issues
Pull requests
Actions
Projects
Security
Insights
master
SPTH / articles / files / LLMorpher.txt
SPTHvx Update LLMorpher.txt
1 contributor
609 lines (447 sloc)
31.2 KB
1
2 **
3 Using GPT to encode and mutate computer viruses
4 entirely in natural language
5
6 by Second Part To Hell
7 **
8
9
10 The ideas and behaviour of a computer virus are conventionally
11 stored as executable code written in a computer language.
12
13 Here we go beyond and show how to encode a self-replicating
14 code entirely in the natural language. Rather than concrete


A-TYPE
LINES-221
TOP
589800
SCORE
C46760
STATISTICS
077
066
078
091
095
073
091
NEXT
LEVEL
28


We are no longer securing computers.
We are securing the society.


「インターネットの敵」とは誰か?
サイバー犯罪の40年史と倫理なきウェブの未来
IF IT'S SMART, IT'S VULNERABLE
MIKKO HYPPONEN
ミッコ・ヒッポネン[著]
安藤貴子[訳]
自由なインターネットは死んだ。あなたのプライバシーも死んだ。
企業も国家も、犯罪者も、私たちの個人情報を狙っている。
最前線でサイバー攻撃の変遷を見てきた30年のキャリアの回想と、
資本主義や公権力が限りなく「スマートで脆弱」にした社会への警鐘。
情報セキュリティの世界的レジェンド、初の日本語訳書
「インターネットの敵」とは誰か?
サイバー犯罪の40年史と倫理なきウェブの未来
ミッコ・ヒッポネン (著), 安藤貴子 (翻訳)
https://www.amazon.co.jp/dp/4575318035/
WITH secure