

Datenanalyse im Kampf gegen Cyberkriminalität - Praktische Anwendungen und Fallstudien

Uncover cybercrime secrets with strategic data analysis.

>_Code blue
by Dussmann

Threat Actor Profiling

Tactics & Techniques

Uncover their attack methods.

Motivations & Goals

Understand their ultimate objectives.

Target Selection

Identify who they're after.



DanaBot
HDD-drive

Пользователь

Joined: Mar 15, 2022
Messages: 46
Reaction score: 20

Jul 10, 2023

Обновленная версия трояна DanaBot. (Аренда) / Updated version of the DanaBot Trojan. (Rent)

Аренда в месяц / Rent per month

Stealer + HVNC = 1000\$

Stealer + PostGrabber = 1000\$

Stealer + PostGrabber + HVNC = 1500\$

Stealer + PostGrabber + HVNC + API + Testing System + Personal Support = 3000\$

Stealer + PostGrabber + HVNC + API + Testing System + Personal Support + Personal Server = (по договоренности / by agreement)

Demo 7 Day (Stealer+HVNC+PostGrabber) = 500\$

Spoiler: Неактуальный тариф

JimmBee

Poison
●●●●●



User
🟢 24

214 posts

Joined

08/23/10 (ID: 32173)

Activity

другое / other

Posted July 10, 2023 (edited)

Обновленная версия трояна DanaBot. (Аренда) / Updated version of the DanaBot Trojan. (Rent)

Аренда в месяц / Rent per month

Stealer + HVNC = **1000\$**

Stealer + PostGrabber = **1000\$**

Stealer + PostGrabber + HVNC = **1500\$**

Stealer + PostGrabber + HVNC + API + Testing System + Personal Support = **3000\$**

Stealer + PostGrabber + HVNC + API + Testing System + Personal Support + Personal Server = (по договоренности / by agreement)

Demo 7 Day (Stealer+HVNC+PostGrabber) = **500\$**

>_Code blue
by Dussmann

Real-Time Detection: Catching Threats as They Happen

1

Anomaly Detection

Advanced algorithms identify and flag suspicious activity in real-time, enabling immediate response.

2

Threat Correlation

Connecting disparate data points to uncover complex, multi-stage cyber attacks as they unfold.

3

Automated Mitigation

Immediate, automated actions to contain and neutralize threats before they can cause significant damage.



Case Study: The Power of Data

1

Breach Detected

Data analysis revealed anomaly.

2

Threat Identified

Attacker's methods were exposed.

3

Defense Deployed

Successful mitigation strategy.



Case Study: The Power of Data



Кот Ученый
Премиум
Premium

Joined: Mar 6, 2024
Messages: 150
Reaction score: 15
Escrow deals: 14



Mar 25, 2024

Austria, Revenue \$5 kk
Access type: VPN
Domain User
AV: sentynel
sector: Grocery Retail

tox: [redacted] 7F120CF082DBD59E99

Prise: 300\$

Проблема в том, что, не рискуя, мы рискуем в сто раз больше.

tox: 0EC [redacted] D383561

 Report



Case Study: The Power of Data

Germany, Revenue \$6 kk
Access type: VPN
Local user
AV: dont know
sector: Manufacturing
Prise: \$800



Case Study: The Power of Data



globe
CD-ROM

User

Joined: Mar 19, 2024
Messages: 11
Reaction score: 6

Oct 15, 2024

Price: 500
Contacts: pm

GEO: Private (European First World Country)
Sector: Hotel
Type of Access: RMM (Full access to CMD and Powershell)
Revenue +9 Million
AV: Sophos

Local Admin
Connected to Hotel Domain.

Price U\$500

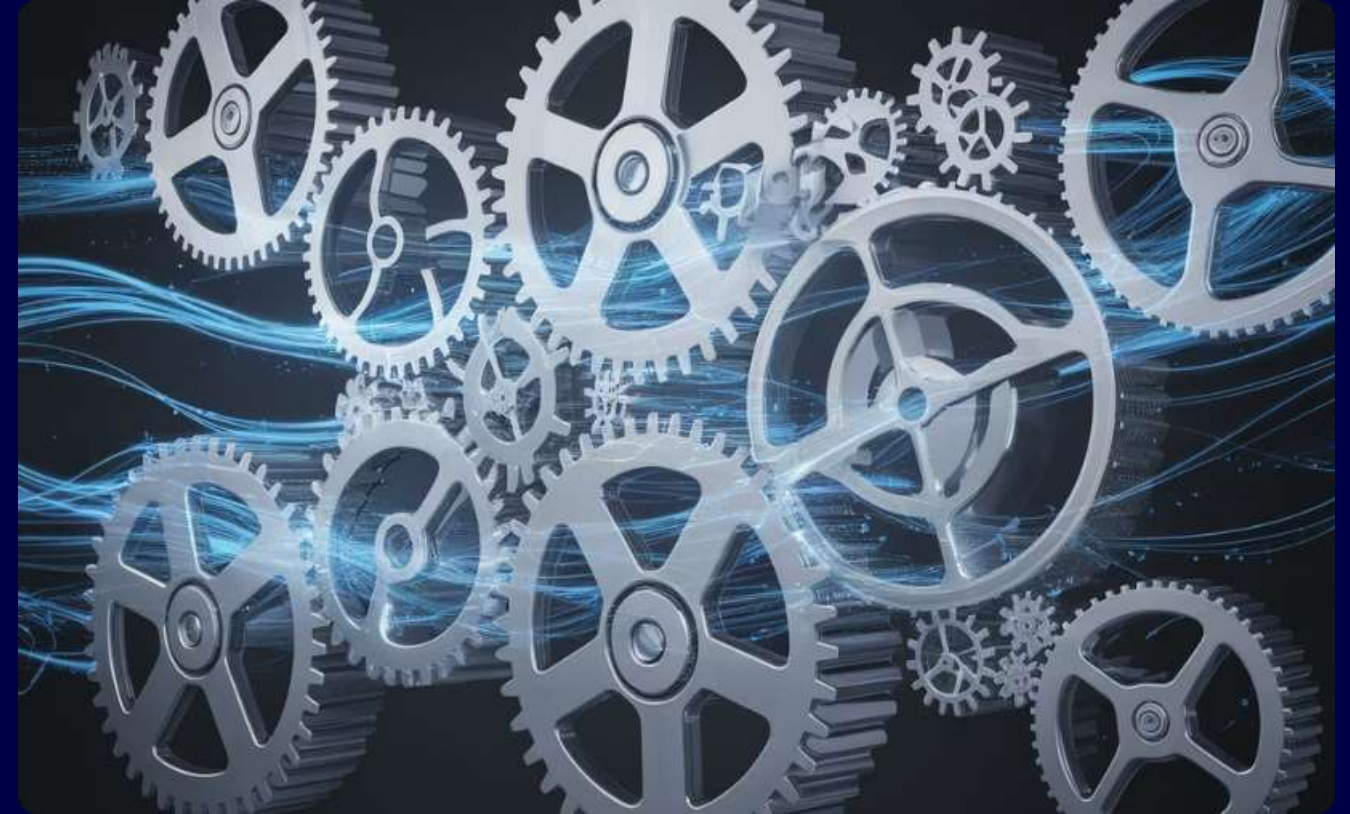


Cutting-Edge Intelligence Tools



AI

Analyzes vast datasets for patterns.



Machine Learning

Adapts and improves over time.

Big Data: Big Impact



Detection

Find threats in massive datasets.



Analysis





















Connect the dots, uncover patterns.

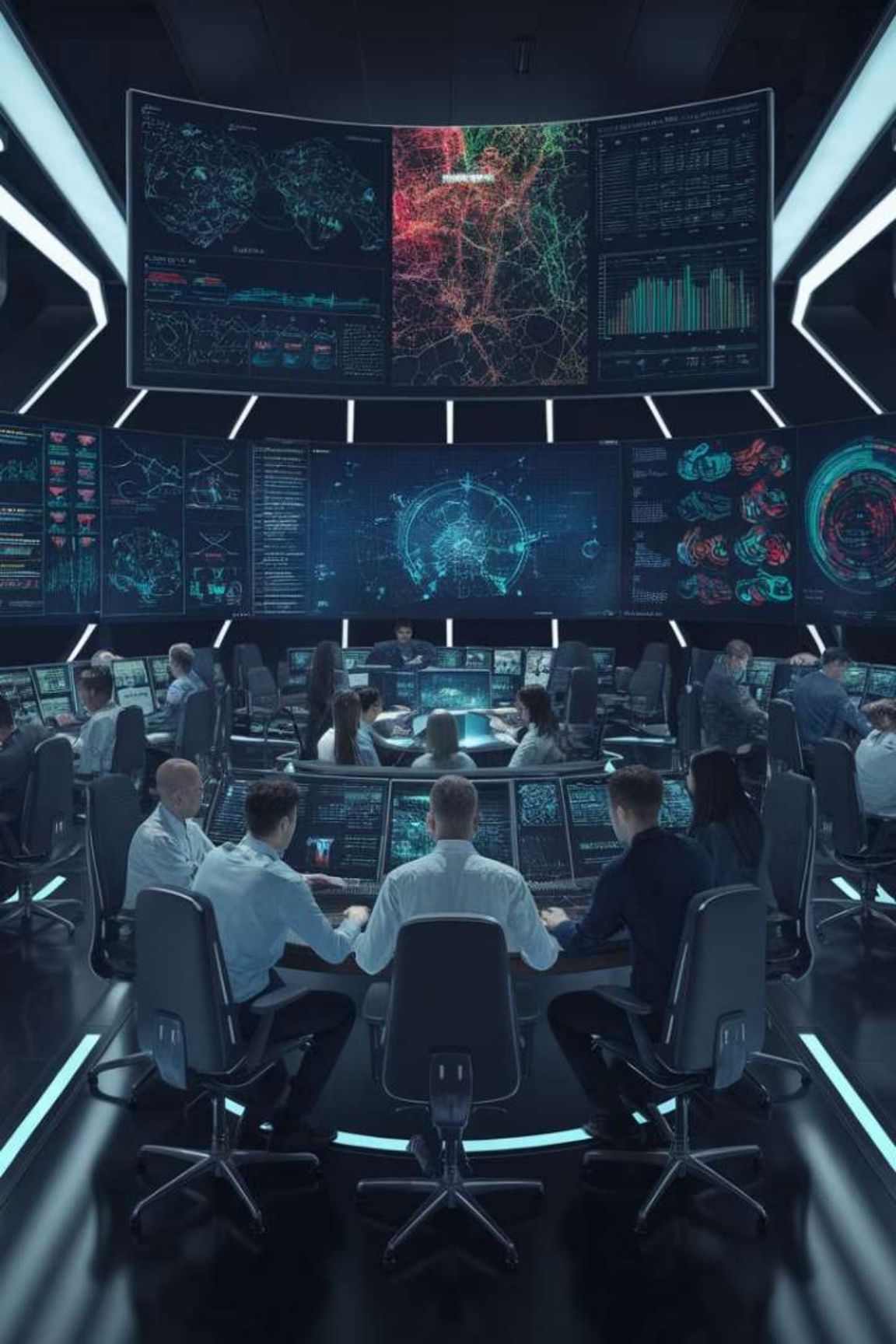


Protection

Strengthen your security posture.

Big Data: Big Impact

Important Threads				
	COLLECTION Over 3.3 Billion unique emails from public leaks and combos (Collected by Addka72424) (Pages: 1 2 3 4 ... 9)	87	7,952	10 hours ago Last Post: UduWynCH0
	How can you earn credits and some other information for new users. (Pages: 1 2 3 4 ... 25)	244	42,490	10-20-2024, 11:45 PM Last Post: d3ff
	Earn credits by reposting leaks! (Pages: 1 2 3)	17	4,247	10-07-2024, 10:44 PM Last Post: hoodlewhoo
	▲ IMPORTANT-READ ▲ Add to official requests (Pages: 1 2)	15	12,841	10-01-2024, 10:13 AM Last Post:  Seacool
	Let's restore the official rf section on the forum together! (Pages: 1 2 3 4 ... 7)	57	100,366	09-29-2024, 02:38 PM Last Post:  readin
Normal Threads				
	www.danto.de 2024	1	87	40 minutes ago Last Post: Boat
	uclss.edu.co fucked	1	173	59 minutes ago Last Post: dunw1ch
	CHECKER MAILACCESS	0	58	1 hour ago Last Post: markhenring17
	Weibo User Database 63,2M lines (REPOST) (Pages: 1 2 3 4 ... 9)	69	19,176	1 hour ago Last Post: rkimeq
	www.dymocks.com.au 2024	0	80	2 hours ago Last Post: MatthewFrida
	 crunchyroll checker working needs proxies 	2	129	2 hours ago Last Post:  Tanaka
	DATABASE: The algerian National Fund for Social Insurance for Workers[Elhanas - Cnas] (Pages: 1 2 3 4 ... 18)	157	13,125	3 hours ago Last Post: chamou8
	79k Indian peopl Cibil Score Including Other Confidential : Pan Number, and loan info	4	365	3 hours ago Last Post: yasbugess
	upac.md - moldova university all dbs LEAKED	3	250	3 hours ago Last Post: wllan45pn
	DATABASE: Twilio Database - Leaked, Download! - 2024 (Pages: 1 2)	15	1,119	3 hours ago Last Post: mazzamozz



Actionable Threat Intelligence

Integrate & Analyze

Use threat data to inform decisions.

Proactive Security

Anticipate and mitigate future attacks.

Stay Informed

Evolving threat landscape awareness.