

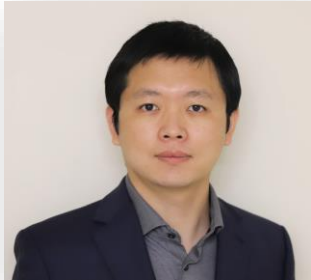


Practical AI and Automation Use Cases for Security Operation

Peter Luo
Co-founder @ DTonomy & Noise Total



Peter Luo



- Microsoft 365 SOC Team
 - Protect Office 365
 - 5 AI patents
- DTonomy Co-founder
 - Security operation platform empowered by easy automation tool and AI
- Ph.D. in Computer Science

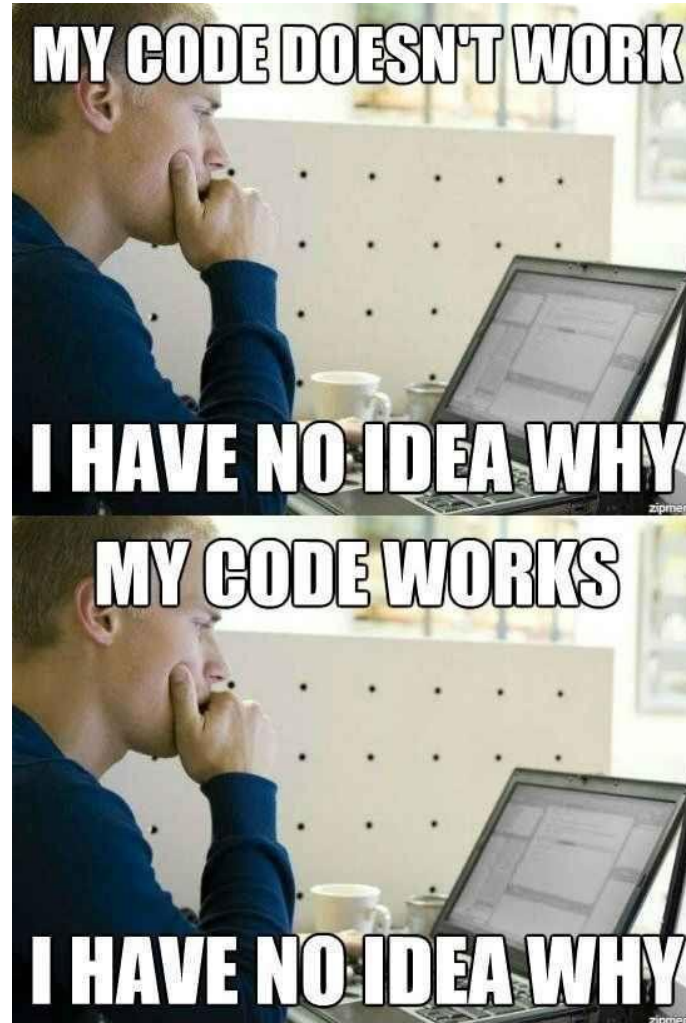
Agenda

- Security Automation High Level
- Security Automation Live Demo
- AI High Level
- AI Demo
- NoiseTotal – Blue Team Intelligence Intro

Develop for SOC @ Microsoft

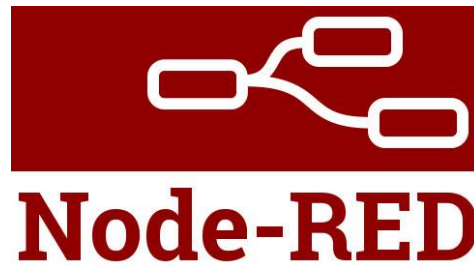


Challenges



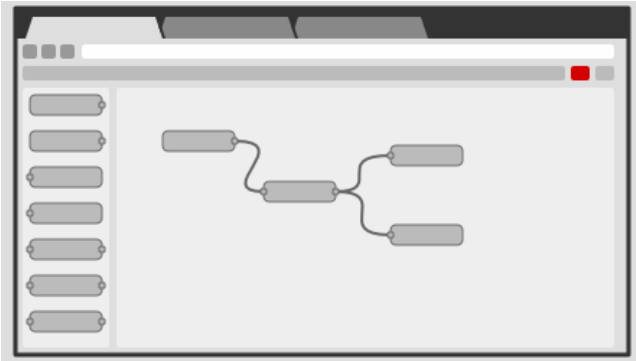
Node-RED - One of the interesting low-code tools

>10,000
Users

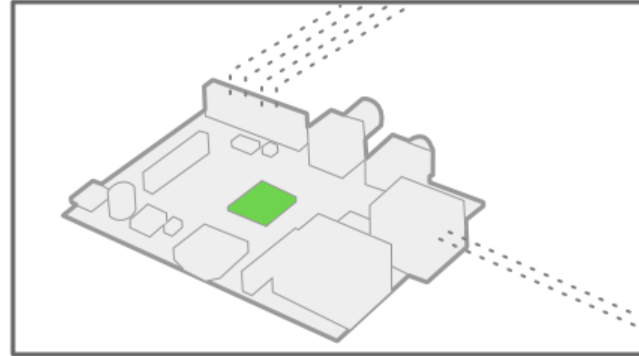


>3,000
3rd party integrations

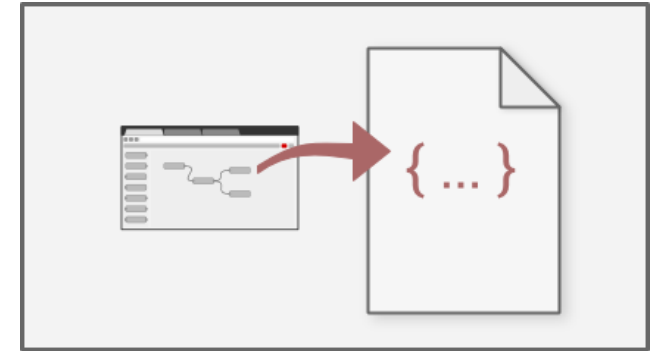
Node-RED high level



Browser-based flow editing



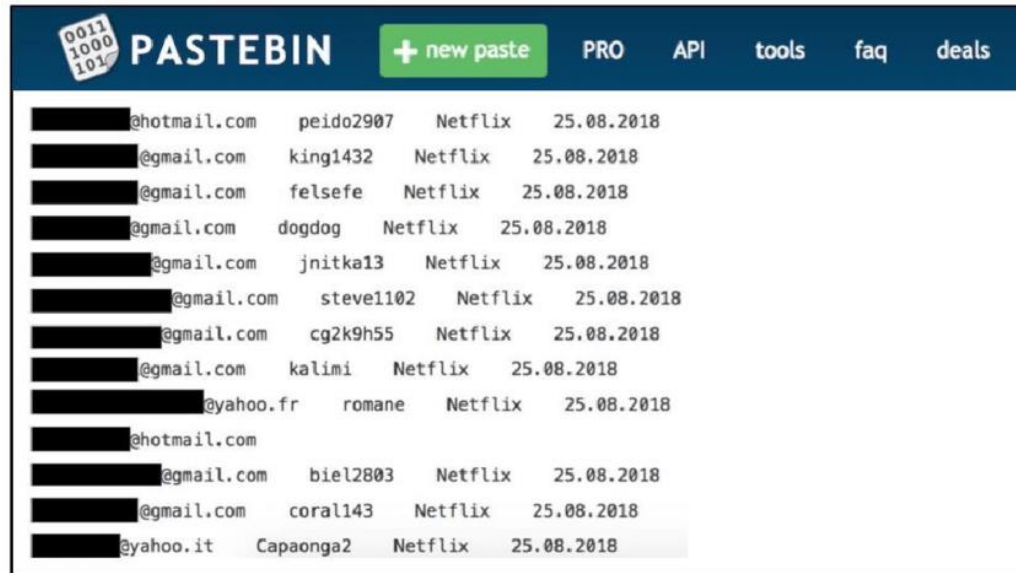
Built on Node.js



Easy Share



Threat Monitoring

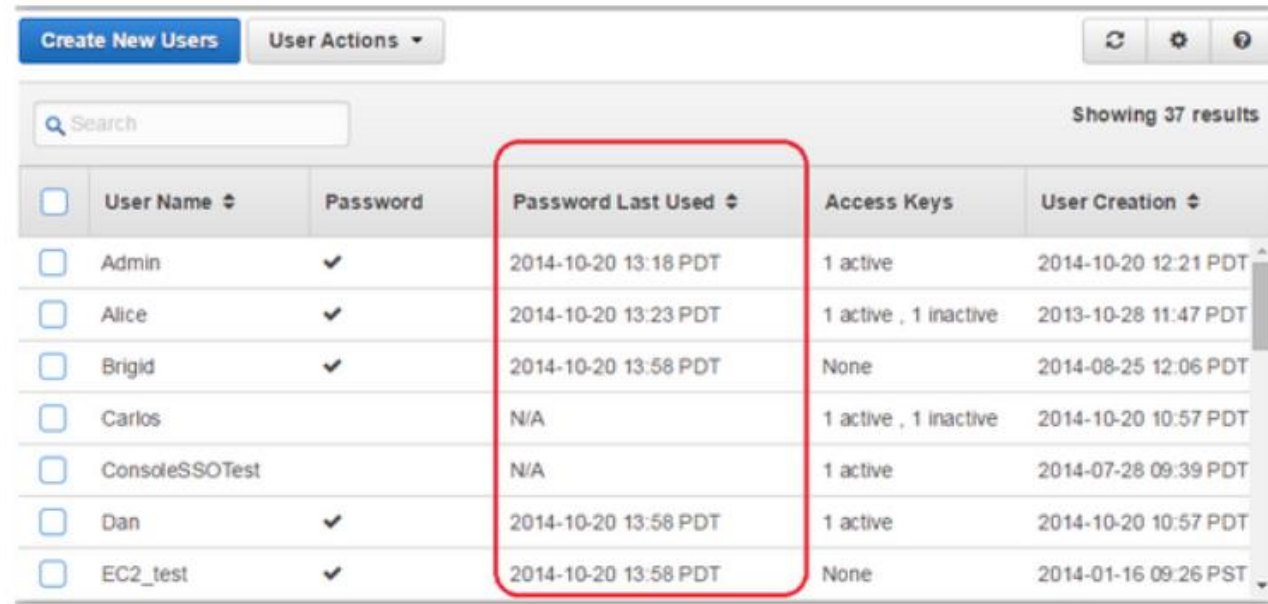


The image shows a screenshot of a Pastebin page. The header includes the Pastebin logo, a '+ new paste' button, and navigation links for 'PRO', 'API', 'tools', 'faq', and 'deals'. The main content is a list of 14 entries, each consisting of a redacted email address, a username, the service name 'Netflix', and the date '25.08.2018'.

Email Address	Username	Service	Date
[redacted]@hotmail.com	peido2907	Netflix	25.08.2018
[redacted]@gmail.com	king1432	Netflix	25.08.2018
[redacted]@gmail.com	felsefe	Netflix	25.08.2018
[redacted]@gmail.com	dogdog	Netflix	25.08.2018
[redacted]@gmail.com	jnitka13	Netflix	25.08.2018
[redacted]@gmail.com	steve1102	Netflix	25.08.2018
[redacted]@gmail.com	cg2k9h55	Netflix	25.08.2018
[redacted]@gmail.com	kalimi	Netflix	25.08.2018
[redacted]@yahoo.fr	romane	Netflix	25.08.2018
[redacted]@hotmail.com			
[redacted]@gmail.com	biel2803	Netflix	25.08.2018
[redacted]@gmail.com	coral143	Netflix	25.08.2018
[redacted]@yahoo.it	Capaonga2	Netflix	25.08.2018

Monitor Data Leaking

Security Auditing



The screenshot shows a user management interface with a table of users. The table has columns for 'User Name', 'Password', 'Password Last Used', 'Access Keys', and 'User Creation'. A red box highlights the 'Password Last Used' column, which contains dates and times for each user. The 'Password' column shows checkmarks for most users, and the 'Access Keys' column shows the number of active and inactive keys for each user.

<input type="checkbox"/>	User Name ↕	Password	Password Last Used ↕	Access Keys	User Creation ↕
<input type="checkbox"/>	Admin	✓	2014-10-20 13:18 PDT	1 active	2014-10-20 12:21 PDT
<input type="checkbox"/>	Alice	✓	2014-10-20 13:23 PDT	1 active , 1 inactive	2013-10-28 11:47 PDT
<input type="checkbox"/>	Brigid	✓	2014-10-20 13:58 PDT	None	2014-08-25 12:06 PDT
<input type="checkbox"/>	Carlos		N/A	1 active , 1 inactive	2014-10-20 10:57 PDT
<input type="checkbox"/>	ConsoleSSOTest		N/A	1 active	2014-07-28 09:39 PDT
<input type="checkbox"/>	Dan	✓	2014-10-20 13:58 PDT	1 active	2014-10-20 10:57 PDT
<input type="checkbox"/>	EC2_test	✓	2014-10-20 13:58 PDT	None	2014-01-16 09:26 PST

Security Analysis

Singapore Specialist : Corona Virus Safety Measures



Tuesday, 28 January 2020 at 03:51

[Show Details](#)

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus. This little measure can save you.

Use the link below to download

[Safety Measures.pdf](#)

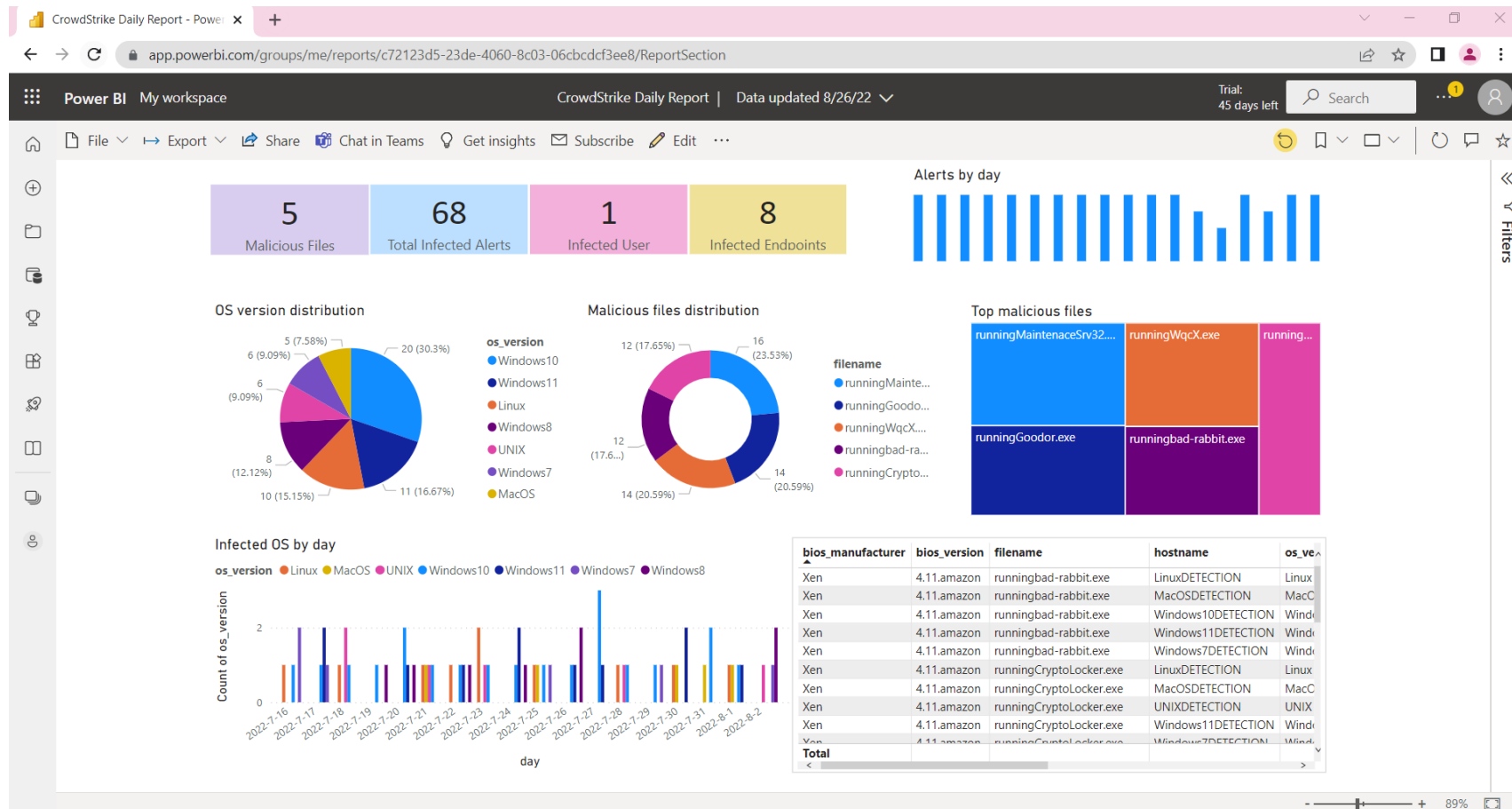
Symptoms Common symptoms include fever, cough, shortness of breath, and breathing difficulties. I

Regards

Dr [Redacted]
Specialist wuhan-virus-advisory

[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]

Reporting



Firewall Management

Add a Firewall Rule

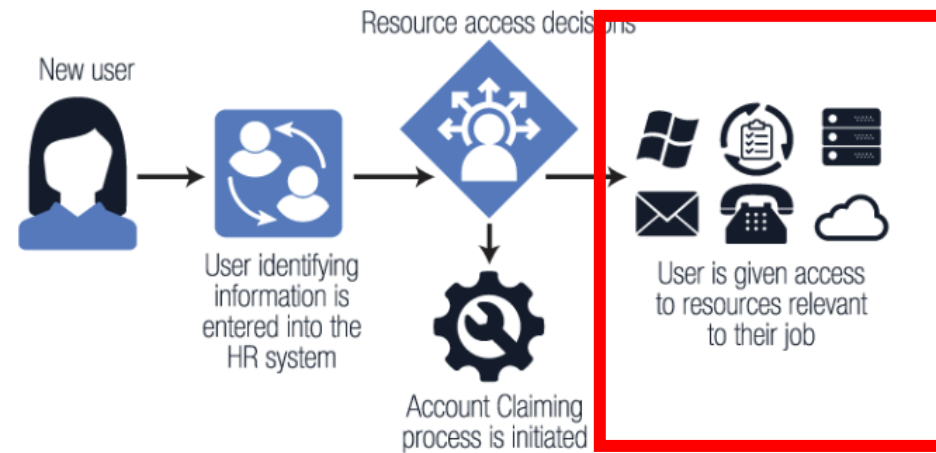
```
PS C:\> New-NetFirewallRule -Action Allow  
-DisplayName Pentester-C2 -RemoteAddress  
<IPADDR>
```

Add a firewall rule to the built-in Windows firewall.

Usage scenario: Allow connections into a new port for a listening backdoor, a service ready to deliver an exploit to clients, or a pivot.

Administrative Tasks

The onboarding process







Simple & repetitive tasks

Prebuilt procedural automation is GREAT!

AI – Augmented Intelligence

Goes Beyond Simple Automation!

AI (LLM) – The rising of ChatGPT

$$P_{\theta}(\overset{\text{next element}}{X_{t+1} = x_{t+1}} \mid \overset{\text{history}}{x_1, \dots, x_t})$$

AI for Security Use Cases

- Write SIEM Query
- Generate Security Detections
- Write Security Policy
- Identify Vulnerability
- Write Automation Policy
- Assist Incident Response
- ...

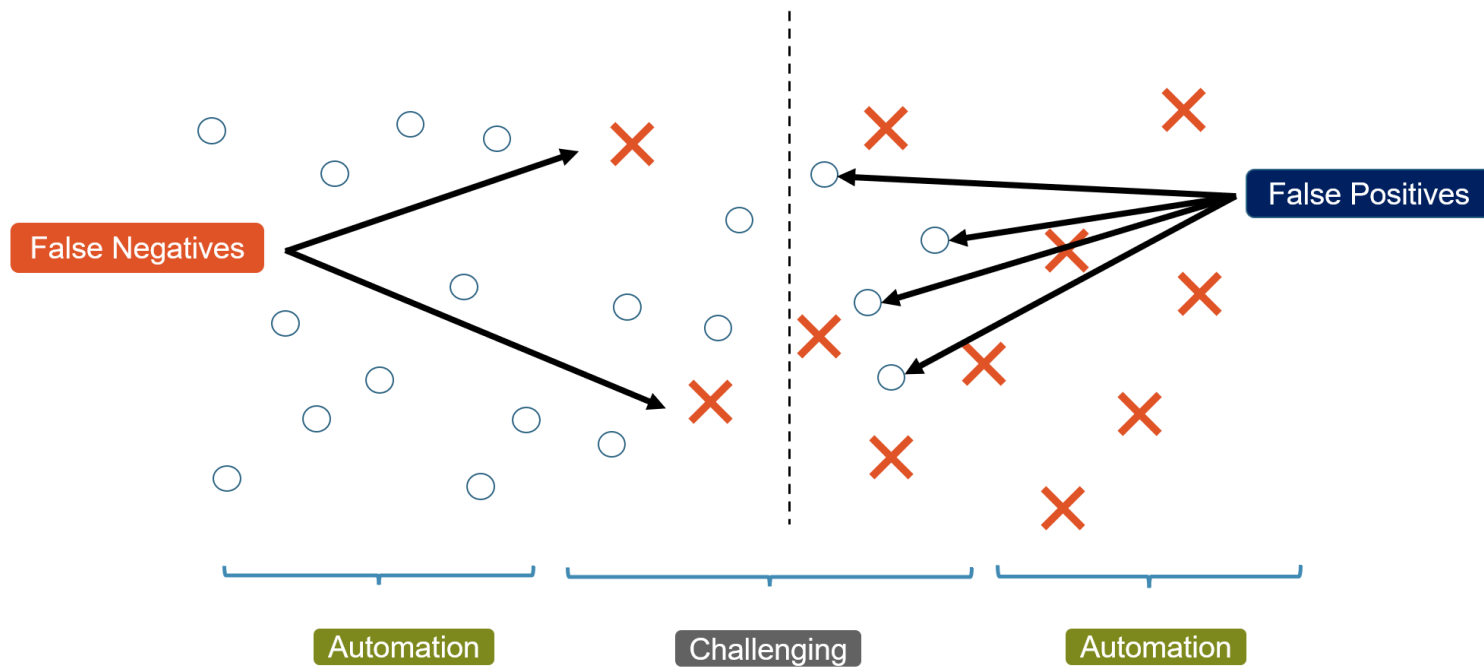
Combine Automation And AI

- Demo

AI Trains on Large Data

Need Human Intelligence to Solve Challenging Problems!

For example: Identify false positives



← Tweet



Florian Roth ⚡
@cyb3rops

After years in security monitoring, detection engineering, training ML models and writing detections, you'll learn one thing:

The problem isn't that malware tries to look like legitimate software, it's that software does a lot of things that you'd only expect from malware

21:20 · 31 Jan 23

Noise Total – Community Intelligence for Blue Team

The opposite of Virus Total



Noise Total

Collective intelligence on false positives in security detections.

[+Contribute](#) · [Sign In](#)

Posts

Tags 96 separate filters by space

Hot Pinned **Newest** Most Votes

- 1 | **McAfee found Virus in Steam client**
| McAfee Steam · last edit Sep 29, 2022 by **cactus** 0 0 0
- 2 | **Samsung said the pre-installed spyware was a false posi...**
| Samsung VIPRE · last edit Sep 28, 2022 by **cactus** 0 0 0
- 3 | **GitHub Desktop installer page was blocked by Bitdefender**
| bitdefender ESET GitHub f-secure · last edit Sep 27, 2022 by **cactus** 0 0 0
- 4 | **Antiy-AVL detected a trojan from Pure Browser**
| Antiy Pure Browser · last edit Sep 21, 2022 by **cactus** 0 0 0
- 5 | **Game downloaded from the RARGB was detected malicious**
| microsoft defender · last edit Sep 21, 2022 by **cactus** 0 0 0

Summary

- Try Node-RED, start automating boring tasks
- Exciting moment with AI – More innovations are coming!
- Noise Total – Call for contribution!



Peter Luo

pchluo@dtonomy.com

www.dtonomy.com

Twitter: @NoiseTotal

NOISE.TOTAL.

Dtonomy